Citrix DaaS™

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Overview 94
Introduction 94
Site overview 94
Components and services managed by Citrix 95
Studio 96
Components and technologies managed by the customer 101
Objects you configure to deliver desktops and applications 103
Citrix Managed Azure 104
Ordering Citrix Managed Azure 105
Citrix Managed Azure benefits summary 105
Delivering applications and desktops to users 106
Citrix® StoreFront and Citrix® StoreFront Cloud 106
Citrix Workspace app 106
Service Level Agreement 107
Limitations 107
More information 107
Get started 108
What's new 109
What's new 109
Virtual Delivery Agents (VDAs) 109
August 2026 110
New and enhanced features 110
July 2026 111
New and enhanced features 111
June 2026 114
New and enhanced features 114

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Image management support prepared image searching 115

Support for creating Citrix Provisioning catalogs in OpenShift virtualization environments using Studio 116

Support for creating Citrix Provisioning catalogs in Citrix Web Studio for Nutanix AHV Prism Central 116

May 2026 116

New and enhanced features 116

April 2026 118

New and enhanced features 118

March 2026 125

New and enhanced features 125

February 2026 127

New and enhanced features 127

January 2026 132

New and enhanced features 132

December 2025 134

New and enhanced features 134

November 2025 136

New and enhanced features 136

October 2025 139

New and enhanced features 139

September 2025 142

New and enhanced features 142

August 2025 145

New and enhanced features 145

July 2025 151

New and enhanced features 151

June 2025 157

© 1997–2026 Citrix Systems, Inc. All rights reserved.

New and enhanced features 157
May 2025 164
New and enhanced features 164
April 2025 167
New and enhanced features 167
March 2025 171
New and enhanced features 171
February 2025 176
New and enhanced features 176
January 2025 179
New and enhanced features 179
December 2024 183
New and enhanced features 183
November 2024 190
New and enhanced features 190
October 2024 194
New and enhanced features 194
September 2024 198
New and enhanced features 198
August 2024 201
New and enhanced features 201
July 2024 206
New and enhanced features 206
June 2024 219
New and enhanced features 219
May 2024 222
New and enhanced features 222
April 2024 227

© 1997–2026 Citrix Systems, Inc. All rights reserved.

New and enhanced features 227
March 2024 230
New and enhanced features 230
February 2024 231
New and enhanced features 231
January 2024 235
New and enhanced features 235
December 2023 237
New and enhanced features 237
November 2023 238
New and enhanced features 238
October 2023 245
New and enhanced features 245
September 2023 248
New and enhanced features 248
August 2023 249
New and enhanced features 249
July 2023 253
New and enhanced features 253
June 2023 254
New and enhanced features 254
May 2023 258
New and enhanced features 258
April 2023 262
New and enhanced features 262
March 2023 265
New and enhanced features 265
February 2023 267

© 1997–2026 Citrix Systems, Inc. All rights reserved.

New and enhanced features 267
January 2023 269
New and enhanced features 269
December 2022 270
New and enhanced features 270
November 2022 271
New and enhanced features 271
October 2022 273
New and enhanced features 273
September 2022 274
New and enhanced features 274
August 2022 275
New and enhanced features 275
July 2022 277
New and enhanced features 277
June 2022 279
New and enhanced features 279
May 2022 281
New and enhanced features 281
April 2022 283
New and enhanced features 283
March 2022 288
New and enhanced features 288
February 2022 289
New and enhanced features 289
January 2022 291
New and enhanced features 291
December 2021 293

© 1997–2026 Citrix Systems, Inc. All rights reserved.

New and enhanced features 293
November 2021 294
New and enhanced features 294
October 2021 295
New and enhanced features 295
September 2021 295
New and enhanced features 295
August 2021 298
New and enhanced features 298
July 2021 299
New and enhanced features 299
June 2021 300
New and enhanced features 300
May 2021 302
New and enhanced features 302
April 2021 304
New and enhanced features 304
March 2021 306
New and enhanced features 306
February 2021 309
New and enhanced features 309
January 2021 311
December 2020 313
New and enhanced features 313
October 2020 314
New and enhanced features 314
September 2020 316
New and enhanced features 316

© 1997–2026 Citrix Systems, Inc. All rights reserved.

August 2020 316
New and enhanced features 316
July 2020 318
New and enhanced features 318
May 2020 319
New and enhanced features 319
April 2020 319
New and enhanced features 319
March 2020 320
New and enhanced features 320
January 2020 322
New and enhanced features 322
December 2019 323
New and enhanced features 323
November 2019 323
New and enhanced features 323
October 2019 324
New and enhanced features 324
September 2019 324
New and enhanced features 324
August 2019 325
New and enhanced features 325
July 2019 325
New and enhanced features 325
June 2019 326
New and enhanced features 326
May 2019 327
New and enhanced features 327

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 2019 327
New and enhanced features 327
January 2019 329
New and enhanced features 329
December 2018 329
New and enhanced features 329
November 2018 329
New and enhanced features 329
Fixes 330
October 2018 330
New and enhanced features 330
September 2018 330
New and enhanced features 330
Fixes 331
August 2018 331
July 2018 334
June 2018 335
May 2018 335
March 2018 335
Fixes 336
January 2018 336
December 2017 337
New and enhanced features 337
November 2017 337
New and enhanced features 337
Fixes 337
More information 338
Known issues 338

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deprecations and removals 339
Deprecations and removals 340
Features in preview 348
List of features in preview 348
Citrix Integration with Azure Local for Linux workload 349
Secure Private Access integration with Monitor 349
Enrollment of Hybrid Entra ID joined non-persistent VMs into Microsoft Intune 349
VUS Multi Release Support 349
Preview to general availability (GA) 350
System requirements 351
Introduction 351
Cloud Connectors 351
Hypervisor connectivity validation 351
Pre-Migration validation 352
Actionable reporting 352
VDAs in an Azure environment 352
VDAs in Amazon WorkSpaces Core Managed Instances 353
VDA for single-session OS 353
VDA for multi-session OS 354
Hosts / virtualization resources 356
Active Directory functional levels 358
HDX technologies 358
Universal Print Server 358
Service connectivity 359
Other 359
Limits 360
Configuration limits 360
Resource location limits 361

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Provisioning limits 361
Usage limits 362
Limits change log 363
Technical security overview 365
Security overview 365
Citrix cloud-based compliance 365
Data flow 366
Data isolation 366
Service editions 366
ICA® Security 366
Basic encryption 367
Secure HDX 367
SecureICA 367
HDX Direct 368
Internal 368
External 368
VDA TLS/DTLS 369
More resources 369
Credential handling 370
Deployment considerations 370
Cloud Connectors 370
Communication with Citrix Cloud 370
HTTPS for XML service and STA 370
Network access requirements 371
Security Keys 371
Client access 371
Client access via Citrix® StoreFront Cloud 372
Client access via Citrix StoreFront 372

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User credentials 372

Connecting to Cloud Connectors using HTTPS 373

XML trust 373

Citrix Gateway service 373

On-premise NetScaler® gateway 374

More information 374

Technical security overview for Citrix Managed Azure 374

Virtual channel allow list 375

Configuration 375

Adding virtual channels to the allow list 375

For single processes 375

For multiple processes 376

Using wildcards 376

Using system environment variables 377

Obtain virtual channel names and processes 377

Considerations for Citrix virtual channels 378

Multimedia Redirection 378

HDX RealTime Optimization Pack for Skype for Business 378

Delivery methods 380

Citrix Virtual Apps published apps and desktops 380

VM hosted apps 382

VDI desktops 383

Remote PC Access 384

Plan and build a deployment 385

How to use this article 385

Plan and prepare 385

Sign up 386

Set up a resource location 386

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a connection to the resource location 387
Install VDAs 387
Create a catalog 388
Create a delivery group 389
Deploy other components and technologies 390
Launch applications and desktops 390
More information 391
Sign up for Citrix DaaS™ 391
Introduction 391
Demos and trials 392
If you currently subscribe to a Citrix DaaS service 392
Order through Citrix 392
Order through Azure Marketplace 393
Requirements for ordering through Azure Marketplace 393
Procedure for ordering through Azure Marketplace 394
After ordering through Azure Marketplace 395
Order through Google Cloud Marketplace 395
What's next 396
Citrix DaaS™ for Microsoft Azure 396
Quick Deploy for Microsoft Azure 396
Differences between Quick Deploy and Studio workflows 397
Citrix HDX™ Plus for Windows 365 399
Citrix DaaS™ Quick Deploy for Amazon WorkSpaces Core Bundles 399
Introduction 399
Prepare and create a deployment 399
Before you start 400
Prerequisites to complete in Citrix Cloud 400
Prerequisites to complete in AWS 400

© 1997–2026 Citrix Systems, Inc. All rights reserved.

General preparation 401
Create a resource location 401
Connect your AWS account 402
Create AssumeRole for Amazon WorkSpaces Core integration 404
(Optional) Set up BYOL for your account 407
Create a directory connection 409
Import an image 410
Requirements for Dedicated Tenancy Images 411
Requirements for Default or Shared Tenancy Images 412
OS, Directory Type, and Session Support Compatibility 413
Integrate Microsoft Office 2019 Image when importing an image 413
Create a custom image from an existing WorkSpaces instance 414
Create a deployment 417
Integrate Microsoft 365 Windows apps 419
Manage machines in a deployment 419
Add applications to a deployment 419
Use persistent desktops with a non-persistent user profile 420
Reference 420
AWS account programmatic access permissions 420
Citrix DaaS™ for Google Cloud 424
Quick Deploy for Google Cloud 425
Launch Quick Deploy for Google Cloud 425
Manage user access rights 426
Convert a deployment 427
Use DaaS get-started guide 428
Benefits 428
Supported deployment scenarios 428
Terminology 429

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access the guide 430
Deliver apps and desktops from scratch (power managed) 430
Prerequisites 431
Preparation 431
Deployment steps 432
Deliver apps and desktops using existing machines (power managed) 436
Prerequisites 436
Preparation 436
Deployment steps 437
Deliver apps and desktops using existing machines (not power-managed) 438
Prerequisites 439
Preparation 439
Deployment steps 439
Deliver office PCs (power managed) 441
Prerequisites 441
Preparation 441
Deployment steps 442
Deliver office PCs (not power-managed) 443
Prerequisites 443
Preparation 443
Deployment steps 444
Machine identities 445
Machine identity types 445
Supported Configurations 446
Supported infrastructure 446
Supported Citrix® StoreFront Cloud authentication identity providers 447
Active Directory joined 447
Microsoft Entra joined 448

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements 448
Limitations 448
Considerations 449
VDA installation and configuration 450
Where to go next 451
Microsoft Intune 451
Requirements for Microsoft Entra joined catalogs enrolled in Microsoft Intune 452
Limitations for Microsoft Entra joined catalogs enrolled in Microsoft Intune 453
Considerations for Microsoft Entra joined catalogs enrolled in Microsoft Intune 453
Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune 453
Prerequisites for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune 453
Requirements for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune 453
Limitations for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune 454
Where to go next 455
Microsoft Entra hybrid joined 455
Requirements 455
Limitations 456
Considerations 456
Where to go next 458
Non-domain-joined 458
Requirements 458
Limitations 458
VDA installation and configuration 459
Where to go next 460
Session authentication 460
Microsoft Entra single sign-on 460
Supported infrastructure 460
Supported identity providers 461

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported access methods 461
System requirements 462
Considerations 463
How to configure Microsoft Entra single sign-on 464
Troubleshooting 481
Microsoft Entra single sign-on Azure configuration 483
Federated Authentication Service 491
Smart cards 491
Web sign-in 492
System requirements 492
How to configure web sign-in 492
How to use web sign-in 493
Set up resource locations 494
Host requirements 495
Active Directory 496
Cloud Connectors 496
Size and scale considerations 496
Add a resource type 497
Activate an unused domain 498
Where to go next 498
Amulet Hotkey CoreStation virtualization environments 498
Key steps 499
Where to go next 499
More information 499
AWS virtualization environments 499
Task overview 501
Task 1: Set up the VPC 501
Task 2: Configure security groups 502

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Task 3: Launch instances 504
Task 4: Create a DHCP options set 505
Task 5: Configure the instances 506
Where to go next 507
More information 507
Google Cloud virtualization environments 508
Prerequisites 508
Google Cloud projects 508
Service endpoint URLs 508
Enable Google Cloud APIs 509
Configure and update service accounts 510
Storage permissions and bucket management 517
Enable private Google access 518
Where to go next 518
More information 518
HPE Moonshot virtualization environments 519
Key steps 519
Where to go next 519
More information 519
Microsoft Azure Resource Manager virtualization environments 519
Where to go next 520
More information 520
Microsoft SCVMM virtualization environments 520
Install and configure a hypervisor 520
Install the VMM console 521
Where to go next 521
More information 521
Nutanix virtualization environments 522

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nutanix Prism Central on AHV 522
Nutanix Prism Element on AHV 523
Where to go next 524
More information 524
Nutanix cloud and partner solutions 524
Nutanix AHV Prism Central 524
NC2 for Nutanix Prism Element 530
Where to go next 531
More information 531
Red Hat OpenShift virtualization environments 531
Key steps 531
Set up your Red Hat OpenShift environment 531
Where to go next 534
More information 534
VMware virtualization environments 534
Where to go next 535
More information 535
VMware cloud and partner solutions 535
Azure VMware Solution (AVS) integration 535
Google Cloud VMware Engine 549
VMware cloud on Amazon Web Services (AWS) 556
Where to go next 561
More information 561
XenServer® virtualization environments 561
Where to go next 562
More information 562
Size and scale considerations for Cloud Connectors 562
Recommended processors and storage 563

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Recommended compute configuration for Local Host Cache 564
Summary of test findings 564
Test methodology 566
Test scenarios and conditions 566
Install VDAs 573
Introduction 573
Installation considerations 573
Restarts during VDA installation 575
Restore on install or upgrade failure 575
VDA installers 576
Troubleshoot 577
Citrix Optimizer 577
Customize a VDA 577
Customize the port for communicating with Cloud Connectors 577
Add the VDA port number on Citrix Cloud Connectors 578
Additional Citrix Cloud Connector configuration when using Rendezvous V1 578
Add the VDA port number on VDAs 579
Troubleshooting 580
Other information 581
Where to go next 581
Install VDAs using the command line 581
Introduction 581
Install a VDA from the command line 582
Command-line options to install a VDA 582
Examples: Install a VDA 589
Customize a VDA using the command line 589
Where to go next 590
WebSocket communication between VDA and Delivery Controller™ 590

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How it works 590
WebSocket support 591
Procedure 591
Create and manage connections 591
Introduction 591
Where to find information about connection types 592
Host storage 592
Storage shared by hypervisors 593
Storage local to the hypervisor 593
Create a connection and resources 594
Step 1. Connection 595
Step 2. Storage management 596
Step 3. Storage selection 598
Step 4. Region 600
Step 5. Network 600
Step 6. Summary 600
Edit connection settings 601
Edit a connection 601
Turn maintenance mode on or off for a connection 603
Delete a connection 603
Rename a connection 603
Test a connection 604
Test TLS Certificate 604
View machine details on a connection 604
Manage machines on a connection 604
Edit storage 605
Detect Orphaned Azure resources 606
Connection timers 606

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Edit networks of resources 607
Delete, rename, or test resources 607
Flexible storage location option for VMs 607
Retrieve a list of orphaned resources 609
Limitations 609
Display the list of orphaned resources 609
Display the list of orphaned resources from a subscription id 610
Use WinHttp (netsh) proxy server settings for hosting connection 610
Use cases 610
Changes to the existing workflow or process 611
Prerequisite 611
Configuration steps 611
Where to go next 613
Connection to Amulet Hotkey CoreStation 613
Create a connection 614
Create a connection using Studio 614
Create a connection using PowerShell commands 614
Certificate and thumbprint validation 615
Manage connections 616
Where to go next 618
More information 618
Connection to AWS EC2 618
Prerequisites 618
Define IAM permissions 618
Create a connection 621
Enhanced proxy configuration for AWS host connection 624
Cross-account provisioning 628
Edit a connection 632

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service endpoint URL 636
Required AWS permissions 637
Validate permissions on host connection 653
Where to go next 654
More information 654
Connection to Amazon WorkSpaces Core Managed Instances 654
Prerequisites 654
Add IAM permissions 655
Create a connection 656
Cross-account provisioning 661
Bypass Cloud Connectors for AWS API requests 665
Edit a connection 668
Service endpoint URL 672
Required AWS permissions 673
Where to go next 690
More information 690
Connection to Google cloud environments 690
Add a connection 691
Create a secure environment for GCP managed traffic 692
Specify CMEK global and regional key 698
Required GCP permissions 700
Where to go next 716
More information 716
Connection to HPE Moonshot 716
Create a connection 716
Certificate and thumbprint validation 718
Manage connections 718
Where to go next 720

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More information 720

Connection to Microsoft Azure Resource Manager 720

Create service principals and connections 720

Manage service principals and connections 729

Create a host connection using Azure Managed Identity 743

Manage Azure Managed Identity of an existing hosting connection 749

Azure Extended Zones 750

Use a pre-created network security group 753

Filter empty resource groups 756

Required Azure permissions 758

Configure required Azure host connection permissions 769

Validate permissions on host connection 769

Where to go next 771

More information 771

Connection to Microsoft SCVMM 771

Create a connection 772

Where to go next 772

More information 772

Connection to Nutanix 772

Nutanix AHV Prism Central host connection 773

Nutanix AHV, Nutanix AHV PC, or Nutanix AHV DRaaS host connection 783

Where to go next 784

More information 784

Connection to Nutanix cloud and partner solutions 785

Nutanix AHV Prism Central 785

Nutanix Prism Element 785

Where to go next 787

More information 787

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connection to Red Hat OpenShift 787
Create a connection 787
Create a hosting unit 790
Where to go next 792
More information 792
Connection to VMware 792
Required permissions 793
Add connections and resources 793
Securing connections to the VMware environment 801
Where to go next 803
More information 803
Connection to VMware cloud and partner solutions 803
Where to go next 804
More information 804
Connection to XenServer® 804
Create a connection to XenServer 804
Use IntelliCache™ for XenServer connections 805
Required XenServer permissions 806
Where to go next 807
More information 807
Service accounts 807
Supported service account types 808
Credential protection 808
On-premises Active Directory service accounts 808
Create an on-premises Active Directory service account 809
Perform machines identity-related actions 810
Where to go next 810
Microsoft Entra service accounts 810

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Permissions required for a Microsoft Entra service principal 811
Create a Microsoft Entra service account 811
Migrate Microsoft Entra joined device management to service account 813
Route Microsoft Entra device management and security group management traffic 813
Where to go next 814
Manage service accounts 815
View service account details 815
Rename a service 815
Edit a service account 815
Test a service account 816
Delete a service account 816
Image management 816
Introduction 816
Use cases 817
What is a prepared image? 818
Requirement 819
Limitations 820
Image lifecycle management using Studio 820
Image lifecycle management using PowerShell 820
Understand Images node 822
Create prepared image machine catalogs 825
Where to go next 826
Create catalogs using prepared images in Amazon WorkSpaces Core Managed Instances 826
Key steps 826
Create an image definition and initial image version using Studio 826
Create a prepared image version spec using PowerShell 828
Share prepared images across availability zones and regions 830
Network setting during image preparation 834

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A machine profile-based machine catalog 834
AWS tenancy 834
Flexible billing 835
Create a catalog 836
Create a catalog using Studio 837
Create a catalog using PowerShell 839
MCSIO enabled catalog 846
Encrypt OS and ID disks 853
Enable NitroTPM and UEFI secure boot for VM instances 855
Copy tags on VMs 857
Filter VM instances using PowerShell 857
Where to go next 860
More information 860
Create catalogs using prepared images in AWS EC2 860
Create an image definition and initial image version 860
Share prepared images across availability zones and regions 864
Create a machine catalog 867
Where to go next 870
More information 870
Create catalogs using prepared images in Azure 870
Use Studio 870
Use PowerShell 875
Share prepared images across Azure subscriptions or tenants 886
Share encrypted prepared image across regions, subscriptions, and tenants 887
More information 889
Where to go next 889
Create catalogs using prepared images in Nutanix AHV Prism Central 889
Use PowerShell 889

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More information 891

Where to go next 891

Create catalogs using prepared images in Red Hat OpenShift 891

Use Studio 891

Use PowerShell 894

More information 896

Where to go next 896

Create catalogs using prepared images in VMware 897

Use Studio 897

Use PowerShell 902

More information 907

Where to go next 907

Create catalogs using prepared images in XenServer® 907

Use Studio 907

Use PowerShell 910

More information 915

Where to go next 915

Manage catalogs created using prepared images 915

Use Studio 915

Use PowerShell 917

More information 924

Create machine catalogs 924

Overview 925

RDS license check 926

VDA registration 926

MCS catalog creation summary 926

MCS storage considerations 927

Machine Creation Services (MCS) storage optimization 929

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prepare a master image on the hypervisor or cloud service 930
Volume licensing activation 932
Key Management Service (KMS) 932
Active Directory-based activation (ADBA) 932
Multiple Activation Key (MAK) 932
Create a machine catalog using Studio 934
Launch the catalog creation wizard 935
Select a machine type 935
Select machine management options 936
Select a desktop experience 937
Select an image and a machine profile 938
Configure the machines 940
Security 945
Configure NICs for the machines 945
Add machine accounts 945
Configure identities for machines in the catalog 946
Add domain credentials 950
Select a WEM configuration set for Experience Optimization 951
Upgrade VDA (optional) 952
Review the settings 953
Create an MCS machine catalog using PowerShell commands 954
Assign a specific drive letter to an MCS I/O write-back cache disk 954
Important consideration about setting custom properties 956
Important consideration about setting ProvScheme parameters 956
Add SIDs while creating virtual machines 957
Validate configuration before creating an MCS machine catalog 958
Onboard VMs to Azure Arc 959
Prerequisites 960

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Steps to onboard VM to Azure Arc 960
Considerations 962
Troubleshooting 962
Follow-Me Tagging 963
Advantages 963
Applicability 964
Limitations 964
Important considerations 964
Configure follow-me tagging 965
Use follow-me tagging 966
Troubleshooting 967
Image replication of additional storage for supported on-premises hypervisors 967
Use cases 967
PowerShell commands 968
Where to go next 968
More information 969
Create a catalog of Amazon WorkSpaces Core Managed Instances 969
Prerequistes 969
Network setting during image preparation 970
A machine profile-based machine catalog 970
AWS tenancy 970
Flexible billing 971
Create a catalog 972
Create a catalog using Studio 972
Create a catalog using PowerShell 975
MCSIO enabled catalog 981
Encrypt OS and ID disks 984
Enable NitroTPM and UEFI secure boot for VM instances 986

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Copy tags on VMs 988
Filter VM instances using PowerShell 989
Where to go next 991
More information 992
Create an Amulet Hotkey CoreStation machine catalog 992
Using Studio 992
Where to go next 993
More information 993
Create an AWS EC2 catalog 993
Network setting during image preparation 994
AWS tenancy 994
Tag AWS operational resources 995
Create a catalog 996
Create a catalog using Studio 996
Create a catalog using PowerShell 999
MCSIO enabled catalog 999
Create a machine profile-based machine catalog using PowerShell 1002
Encrypt OS, ID, and WBC disks 1007
Enable NitroTPM and UEFI secure boot for VM instances 1009
Provision a data disk on MCS created VM 1011
Copy tags on VMs 1014
Filter VM instances using PowerShell 1015
Backup SKU list for VMs 1017
Create a catalog using AWS Spot instance 1019
Where to go next 1021
More information 1021
Create a Google Cloud Platform catalog 1021
Prepare a master VM instance and a persistent disk 1021

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable zone selection 1022
Create a machine catalog 1023
Import manually created Google Cloud machines 1027
Shared Virtual Private Cloud 1027
Use Customer Managed Encryption Keys (CMEK) 1033
Uniform bucket-level access compatibility 1035
Use PowerShell 1035
Create a catalog with persistent write-back cache disk 1036
Create a machine catalog using a machine profile 1041
Create a machine catalog with machine profile as an instance template 1042
Create a catalog with shielded VM 1043
Create Windows 11 VMs on the sole-tenant node 1044
VMs and disks with inherited labels 1047
Google Cloud Marketplace 1052
Where to go next 1052
More information 1053
Create an HPE Moonshot machine catalog 1053
Create a machine catalog using Studio 1053
Create a machine catalog using PowerShell commands 1054
Where to go next 1054
More information 1054
Create a Microsoft Azure catalog 1054
Create a machine catalog 1055
Create a machine catalog using an Azure Resource Manager image in Studio 1055
Create an Azure template spec 1069
Export a machine profile to a JSON file 1070
Import a machine profile as an ARM Template spec in Azure 1071
Provision machines into specified Availability Zones 1071

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure ephemeral disks 1072
Azure Compute Gallery 1075
Conditions for Azure temporary disk to be eligible for write-back cache disk 1076
Azure server-side encryption 1077
Azure disk encryption at host 1078
Double encryption on managed disk 1078
Azure resource groups 1079
Azure Marketplace 1080
Provision catalog VMs with Azure Monitor Agent installed 1082
Azure confidential VMs 1083
Boot Integrity Monitoring 1086
Create a catalog of on-demand capacity reservation VMs 1088
Nested virtualization 1090
NVMe-only SKUs 1090
Use PowerShell 1092
Use template spec in creating or updating a catalog using PowerShell 1093
Enable Azure VM extensions 1094
Machine catalogs with Trusted Launch 1094
Use machine profile property values 1100
Configure Availability Zones using PowerShell 1107
Provision VMs on Azure dedicated hosts 1109
Configure storage types 1110
Enable zone-redundant storage 1111
Capture diagnostic settings on VMs and NICs from a machine profile 1113
Verify the Windows license 1116
Configure the Linux license 1116
Create a machine catalog with an Azure ephemeral disk 1117
Configure Azure Compute Gallery 1120

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create or update a catalog with multiple NICs per VM 1123
Create a machine catalog with non-persistent write-back cache disk 1126
Create a machine catalog with persistent write-back cache disk 1127
Improve boot performance with MCSIO 1130
Create a machine catalog with customer-managed encryption key 1131
Create a machine catalog with encryption at host capability 1133
Create a machine catalog with double encryption 1134
Page file location determination 1139
Page file setting scenarios 1139
Specify page file setting 1140
Modify page file settings 1142
Provision catalog VMs with AMA enabled 1143
Create a catalog using Azure Spot VMs 1147
Configure backup VM sizes 1150
Copy tags on all resources 1154
Create a preformatted WBC disk catalog 1156
Delete WBC disk at shutdown for MCS provisioned Citrix Provisioning™ catalogs 1158
Provision data disk 1159
Migrate from unmanaged to managed disks 1161
Where to go next 1164
More information 1164
Create a Microsoft SCVMM catalog 1164
Create a master VM 1165
MCS on SMB 3 file shares 1165
Create catalog with a machine profile 1167
Where to go next 1170
More information 1170
Create a Nutanix catalog 1170

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a machine catalog using Nutanix machine template version 1170
Create a machine catalog with existing machines (power managed) 1181
Create a machine catalog using a Nutanix snapshot 1182
Where to go next 1183
More information 1183
Create a Red Hat OpenShift catalog 1184
Create a master image VM 1184
Create a catalog 1185
Where to go next 1191
More information 1191
Create a VMware catalog 1191
Create a machine catalog using a machine profile 1191
Check for multiple NICs 1197
Provision a Data disk on MCS created VM 1198
Troubleshooting 1200
Where to go next 1200
More information 1200
Create a XenServer® catalog 1200
Create a machine catalog using a GPU-capable XenServer 1200
Create a machine profile-based machine catalog using PowerShell 1201
Where to go next 1204
More information 1204
Identity pools of different machine identity join types 1204
Identity pool of on-premises Active Directory joined machine identity 1204
Use Studio 1204
Use PowerShell 1205
More information 1206
Identity pool of Microsoft Entra joined machine identity 1206

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use Studio 1207
Use PowerShell 1209
View the status of the Microsoft Entra join process 1212
Delivery Group 1213
Enable Rendezvous 1213
Troubleshoot 1213
Microsoft Entra dynamic security groups 1214
Create a Microsoft Entra dynamic security group under an existing Microsoft Entra ID assigned security group 1219
Modify Microsoft Entra dynamic security group name 1224
More information 1225
Identity pool of Microsoft Entra hybrid joined machine identity 1225
Use Studio 1225
Use PowerShell 1227
View the status of the hybrid Microsoft Entra join process 1230
Troubleshoot 1231
Identity pool of Microsoft Intune enabled machine identity 1232
Create Microsoft Entra catalogs enrolled in Microsoft Intune 1233
Create Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune 1237
More information 1242
Identity pool of non-domain-joined machine identity 1242
Use Studio 1243
Use PowerShell 1243
Manage machine catalogs 1244
Introduction 1244
About persistent instances 1245
Manage Machine Catalogs 1245
Use Studio 1245

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View catalog details 1246
Add machines to a catalog 1249
Use CSV files to bulk add machines to a catalog 1250
Enroll machines to catalogs using the WebSocket VDA enrollment tool 1253
Delete machines from a catalog 1256
Edit a catalog 1257
Rename a catalog 1259
Delete a catalog 1259
Manage Active Directory computer accounts in a catalog 1260
Change the master image for a catalog 1261
Convert MCS-provisioned catalogs from using master images to using prepared images 1261
Update or create an image 1261
Change the master image 1262
Rollout strategy 1263
Roll back the master image 1264
Change the functional level or undo the change 1265
Clone a catalog 1265
Organize catalogs using folders 1266
Required roles 1266
Create a catalog folder 1266
Move a catalog 1267
Manage catalog folders 1267
Required permissions 1268
Upgrade VDAs 1268
Manage experience optimization settings for a catalog 1268
Required permissions 1268
Edit the experience optimization settings 1269
Retry catalog creation 1269

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(Non-Citrix provisioned VDAs only) Generate and manage enrollment tokens 1270
Manage tokens 1271
Use PowerShell 1271
Manage the sequence number of the machine name 1272
Add descriptions to an image 1272
Reset OS disk 1273
Repair the identity information of active computer accounts 1275
Conditions 1275
Reset identity information 1276
Change the network setting for an existing machine catalog 1277
Manage versions of a machine catalog 1278
Change cache configuration of an existing machine catalog 1279
Requirements 1280
Change the cache configuration 1280
Convert a non-machine profile-based machine catalog to a machine profile-based machine catalog 1281
Retrieve warnings and errors associated with a catalog 1282
Delete machines without hypervisor access 1283
Limitations 1283
Use the PurgeDBOnly command 1283
Update properties of individual VMs 1284
Update properties of a VM 1285
Retain the properties updated on a VM after the machine catalog is updated 1287
Revert the configuration updates applied to a VM 1288
Storage migration of VMs 1289
Migrate the disk storage 1289
Troubleshoot 1291
Important considerations for migration of non-persistent VMs in VMware 1292

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrate existing MCS provisioned catalogs to prepared image machine catalog 1292
Limitations 1292
Migrate to prepared image machine catalog 1292
Troubleshoot 1293
Where to go next 1293
Manage an AWS EC2 catalog 1294
Remove tags 1294
Identify resources created by MCS 1296
Convert legacy MCS catalogs in AWS to machine profile-based catalogs 1298
More information 1299
Manage a catalog of Amazon WorkSpaces Core Managed Instances 1299
Remove tags 1299
Identify resources created by MCS 1301
More information 1303
Manage a Google Cloud Platform catalog 1303
Add machines to a catalog 1303
Update machines 1303
Roll back a machine update 1304
Power management 1304
Update provisioned machines using PowerShell 1305
Change disk related custom properties of an existing catalog 1307
Protect accidental machine deletion 1309
Identify resources created by MCS 1309
More information 1310
Manage an HPE Moonshot catalog 1311
Power management 1311
More information 1311
Manage a Microsoft Azure catalog 1312

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change the storage type to a lower tier when a VM is shut down 1312
Convert legacy MCS catalogs in Azure to machine profile-based catalogs 1317
Update provisioned machines to current provisioning scheme state 1318
Change disk encryption 1324
Use temporary disk as WBC disk for existing catalogs 1329
Retrieve information for Azure VMs, snapshots, OS disk, and gallery image definition 1330
Retrieve region name information for Azure VMs, managed disks, snapshots, Azure VHD, and ARM templates 1331
Clone an MCS catalog 1332
Identify resources created by MCS 1334
Remove tags 1336
More information 1337
Manage a Microsoft SCVMM catalog 1337
Identify resources created by MCS 1337
More information 1338
Manage a Nutanix catalog 1338
Use Studio 1339
Use PowerShell 1344
Migrate machine catalogs to Citrix-managed Nutanix AHV Prism Central host connection 1347
More information 1351
Manage a VMware catalog 1352
Update provisioned VMs to current provisioning scheme state 1352
Update the folder ID of a machine catalog 1355
Identify resources created by MCS 1358
More information 1358
Manage a XenServer® catalog 1358
Identify resources created by MCS 1359
Retrieve information about provisioning scheme 1359

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Retrieve list of resources created by MCS 1360
More information 1360
Power Management 1361
Power manage Amulet Hotkey CoreStation VMs 1362
More information 1362
Power manage AWS VMs 1362
AWS on-demand provisioning 1362
Instance Hibernation 1363
Power manage Azure VMs 1366
Azure on-demand provisioning 1366
Preserving a provisioned virtual machine when power cycling 1367
Customize power on behavior at storage type change failure 1369
Create hibernation-capable VMs 1371
More information 1384
Power manage Nutanix AHV VMs 1385
Security policies 1385
Security group 1385
Security group in AWS 1386
Security group in Microsoft Azure 1386
Security group in Google Cloud Platform 1386
Secure Boot and vTPM 1387
Secure Boot and NitroTPM in AWS 1387
Secure Boot and vTPM in Google Cloud Platform 1387
Secure Boot and vTPM in Microsoft Azure 1388
Secure Boot and vTPM in Nutanix Prism Central 1388
vTPM in VMware 1389
Secure Boot and vTPM for XenServer® 1389
Secure Boot and vTPM in SCVMM 1389

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Encryption capabilities 1389
Encryption capabilities in AWS 1390
Encryption capabilities in Google Cloud Platform 1390
Encryption capabilities in Microsoft Azure 1390
Service Window 1391
Advantages 1392
Improved user experience and continuity 1392
Advanced hardware flexibility 1392
Important consideration 1392
Limitataion 1392
Service Window operations 1392
Reset OS disk 1393
Example: Reset OS disk for specific VMs 1393
Example: Reset OS disk for the entire catalog 1393
Update hardware settings 1393
Important considerations 1394
Schedule hardware updates on an entire machine catalog or new VMs 1394
Schedule hardware updates on specific VMs 1395
Miscellaneous PowerShell commands associated with Service Window 1396
Load balance machines 1397
Load balancing setting at site level 1398
Load balancing setting at delivery group level 1399
Load management 1399
Create delivery groups 1400
Introduction 1400
Before you begin 1400
Pages of the Wizard 1400
Machines page 1402

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Important considerations 1402
Machine Allocation page 1403
Load Balancing page 1403
Delivery Type page 1404
Users page 1404
How user access control works 1407
Configuration steps 1408
Applications page 1410
Important considerations 1411
Configuration steps 1412
Desktops (or Desktop Assignment Rules) page 1412
App Protection page 1414
Scopes page 1414
License assignment page 1415
Policy Set page 1415
Local Host Cache mode page 1415
One-time use pooled desktops in Local Host Cache 1415
Summary page 1417
Limitation 1417
More information 1417
Manage delivery groups 1417
Introduction 1417
General 1418
View group details 1418
Change preferred properties 1419
Change the delivery type of a delivery group 1420
Change StoreFront addresses 1421
Change the functional level 1421

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage Remote PC Access delivery groups 1422
Change the license for a delivery group 1422
Organize delivery groups using folders 1422
Move a delivery group 1424
Manage delivery group folders 1424
Manage app protection 1425
Change suspend capability for a delivery group 1426
Users 1427
Add or remove users in a delivery group 1427
Manage user assignments for Citrix Cloud Library-managed delivery groups 1427
Restrict access to desktops and apps in a delivery group 1428
Restrict access to resources in a delivery group 1429
Restrict user access to resources across all delivery groups 1434
Configure user scope for an access policy 1435
Machines 1435
Manage user assignments for machines 1436
Enable Local Host Cache for single-session pooled VDAs 1437
Update a machine in a delivery group 1438
Add, change, or remove a tag restriction for a desktop 1438
Remove a machine from a delivery group 1439
Prevent users from connecting to a machine (maintenance mode) in a delivery group 1439
Shut down and restart machines in a delivery group 1440
Create and manage restart schedules for machines in a delivery group 1441
Enable a one-time restart schedule 1446
Manage Autoscale 1449
Sessions 1449
Log off or disconnect a session, or send a message to delivery group users 1449
Configure session prelaunch and session linger in a delivery group 1450

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure session roaming 1454
Control session reconnection when disconnected from machine in maintenance mode 1455
Applications 1455
Troubleshoot 1456
Create application groups 1456
Introduction 1456
Example configurations 1457
Example 1 1457
Example 2 1458
Guidance and considerations 1458
Session sharing with application groups 1459
Session sharing between application groups 1460
Disable session sharing within an application group 1461
Create an application group 1461
Step 1. Delivery groups 1462
Step 2. Users 1463
Step 3. Applications 1463
Step 4. Scopes 1464
Step 5. Summary 1465
Manage application groups 1465
Introduction 1465
Enable or disable an application group 1465
Enable or disable application session sharing between application groups 1466
Disable application session sharing within an application group 1466
PowerShell cmdlet examples 1467
Considerations 1467
Rename an application group 1467
Add, remove, or change the priority of delivery group associations with an application group 1468

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add, change, or remove a tag restriction in an application group 1468
Add or remove users in an application group 1469
Add, change, or remove an application icon in an application group 1469
Limitation 1470
Change scopes in an application group 1470
Delete an application group 1470
Organize application groups using folders 1471
Required roles 1471
Create and manage folders 1472
Remote PC Access 1472
Considerations 1474
Deployment considerations 1474
Machine catalog considerations 1475
Linux VDA considerations 1475
Technical requirements and considerations 1476
Configuration sequence 1477
Features managed through the registry 1479
Sleep mode (minimum version 7.16) 1479
Session management 1479
Wake on LAN 1480
Limitation 1481
System requirements 1481
Configure Wake on LAN 1481
Design considerations 1484
Operational considerations 1484
Troubleshoot 1485
Monitor blanking not working 1485

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session disconnects when you select Ctrl+Alt+Del on the machine that has session management notification enabled 1485
Diagnostic information 1486
Power management 1486
The active remote session records the local touchscreen input 1486
More resources 1487
Standalone Citrix Secure Ticketing Authority (STA) service 1487
Standalone STA service scenarios and configuration requirements 1487
Remove components 1487
Remove components using the Windows feature for removing or changing programs 1488
Remove a VDA using the command line 1488
User personalization layer 1488
Application support 1489
Exceptions 1489
Applications that require a local user or administrator account 1490
Requirements 1490
Set up your file share 1491
Recommendations 1491
Microsoft System Center Configuration Manager (SCCM) 1491
User layer size 1491
Tools for overriding the User Layer Size (Optional) 1491
Deploy a User personalization layer 1492
Step 1: Verify that the Citrix Virtual Apps and Desktops environment is available 1492
Step 2: Prepare your master image 1493
Step 3: Create a machine catalog 1495
Step 4: Create a delivery group 1498
Step 5: Create delivery group custom policies 1498
Configure security settings on the user layer folder 1504

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User layer messages 1505

Log files to use when troubleshooting 1505

Limitations 1506

Backup or Migrate your configuration 1508

Backup 1508

Migration 1509

Backup and Restore configuration 1510

Type of backups 1512

Backup and Restore using Studio 1512

Create on-demand backups 1512

Pin a backup 1513

Create scheduled backups 1513

Limit scheduled backups 1513

Auto-pin scheduled backups 1514

Restore 1514

History 1517

Backup and Restore using the Automated Configuration tool 1517

Automated Configuration tool for migration 1518

Automated Configuration tool for backup and restore 1521

Best practices for backup and restore 1521

FAQ 1522

Migrate configuration to Citrix Cloud™ 1523

Known limitations 1523

Prerequisites for migrating your configuration 1523

Key steps 1524

Download Automated Configuration 1525

Upgrade Automated Configuration 1525

Generate the customer ID, client ID, and secret key 1525

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Populate customer info file 1526
Populate zone mapping file 1528
Update the security file for host connections 1528
Per-hypervisor security information 1529
Special security considerations 1530
Export your Citrix Virtual Apps and Desktops on-premises configuration 1530
Supported migration objects 1530
Export on-premises configuration 1531
Import your configuration to Citrix DaaS 1532
Component migration order 1532
Run an import 1534
Understand import operation 1534
Granular migration 1535
Activate sites 1535
Import and transferring control to the cloud 1535
Transfer control back to the on-premises site 1536
Additional site activation information 1536
Understand migrating Machine Creation Services provisioned catalogs 1537
Pooled VDI / multi-session catalogs 1537
Static VDI catalogs 1538
Update MCS tags to detect orphaned resources after migration 1538
Merge multiple sites into a single site 1539
Prefix and suffix rules 1540
Export on-premises site 1541
Merge the sites 1550
Remove a component using the site prefix 1550
Migrate from cloud to cloud 1551
Prerequisites for migrating your configuration 1552

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Back up your Citrix DaaS configuration 1552
Restore your configuration to Citrix DaaS 1553
Activate sites 1554
Migrate Cloud configurations to on-premises 1555
Pre-requisites for migrating your configuration 1555
Key steps 1555
Automated configuration tool cmdlets for migration 1557
Basic cmdlets 1561
On-premises to cloud cmdlets 1561
Cloud to cloud cmdlets 1570
Other basic cmdlets 1575
Granular migration parameters 1577
Migrate by components 1577
Filtering by object names 1577
Prerequisites-related cmdlets 1579
Prerequisites-related parameters 1583
Support and troubleshooting cmdlets 1584
Site activation cmdlets 1588
Merging multiple on-premises sites cmdlets 1591
Site merging parameters 1593
Generic parameters 1594
Cloud accessing parameters 1594
Migration mode parameters 1594
Log display parameters 1595
Cmdlet return values 1595
ActionResult 1595
CustomResult 1596
PowerShell help 1598

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Automated configuration tool cmdlets for backup and restore 1598
Backup storage cmdlets 1598
Get-BckRstrStorage 1598
Set-BckRstrStorage 1599
Test-BckRstrStorage 1601
Back up cmdlets 1602
Get-BckRstrBackups 1602
Get-BckRstrBackupsMembers 1603
New-BckRstrBackup 1605
Pin backups cmdlets 1606
Set-BckRstrPinBackups 1606
Set-BckRstrUnpinBackups 1607
Remove backup cmdlet 1607
Remove-BckRstrBackup 1607
Scheduled backups cmdlets 1608
Get-BckRstrSchedules 1608
New-BckRstrSchedule 1609
Set-BckRstrSchedule 1611
Set-BckRstrScheduleEnabled 1612
Set-BckRstrScheduleDisabled 1613
Limit backups cmdlet 1614
Set-BckRstrOptions 1614
Restore cmdlet 1615
Restore-BckRstrBackups 1615
History cmdlets 1616
Get-BckRstrHistory 1616
Get-BckRstrSpecificBackupHistory 1617
Set-BckRstrNotes 1618

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot Automated configuration and additional information 1619
Automated configuration tool errors 1619
OnErrorAction parameter 1619
Migration cmdlets 1620
Resume parameters 1620
Setting the OnErrorAction in the CustomerInfo.yml file 1621
Logs 1621
Diagnostic files 1622
Export 1622
Import, Merge, Restore, Sync, Backup, Compare 1622
Problems resulting from dependencies 1623
Recommendations 1623
Folders 1623
Default folder root location 1623
Export 1624
Import/Merge/Sync/Compare 1624
Restore 1624
Backups 1624
Changing the default root folder 1625
Files copied to subfolders 1625
Automated fail-safe cloud site backups 1625
Automation 1625
Exporting from PCs other than the Delivery Controller™ 1626
Moving to Citrix Cloud™ Government and Japan Control Plane 1626
Citrix Cloud data collection 1627
Additional resources 1627
Discussion forum 1627
Video 1627

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Training 1627
Print 1628
Install the Universal Print Server on your print servers 1628
Policies 1630
Overview 1631
Tools for managing policies 1631
Policy processing order 1632
Learn about the Studio > Policies interface 1633
Policy configuration workflow 1634
Create templates 1634
Built-in templates 1634
Create templates 1636
Create policies 1637
How policies work 1637
The Unfiltered policy 1638
Assignment modes 1638
Policy settings: Parent-child relationships 1639
Policy setting states 1640
Secure default settings 1641
Policy setting effectiveness 1641
Best practices 1642
Create policies from scratch 1642
Step 1: Select and configure policy settings 1642
Step 2: Specify policy assignments 1643
Create policies from templates 1646
Where to go next 1646
Create policy sets 1646
Benefits 1646

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How it works 1647
Enable policy sets 1648
Create policy sets 1648
Create policy sets from scratch 1649
Clone policy sets 1649
Prioritize policies 1649
Change policy priority using Web Studio 1650
Manage policy assignment exceptions 1650
Use Deny mode for exceptions 1650
Related content 1651
Simulate and evaluate policies 1651
Compare policies and templates 1651
Run the Policy Modeling wizard 1652
View and manage modeling results 1652
Review the report 1652
Manage the report 1652
Evaluate policy application using Resultant Set of Policy 1652
Troubleshoot policy issues 1653
View applied policies in Director 1654
Policy settings reference 1654
HDX™ overview 1655
At the device 1657
On the network 1657
In the data center 1657
HDX Insight 1657
Enable or disable HDX Insight virtual channel 1658
Experience HDX capabilities from your virtual desktop 1658
Auto client reconnect and session reliability 1660

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX adaptive throughput 1661
Improve the image quality sent to user devices 1662
Improve video conference performance 1662
Network traffic priorities 1663
Show or hide the remote language bar 1664
Unicode keyboard mapping 1665
Enable or disable Unicode keyboard layout mapping 1665
Enable Unicode keyboard layout mapping compatible mode 1665
Citrix ICA® virtual channels 1667
What are ICA virtual channels? 1667
64-bit compatibility 1670
Generic USB virtual channel 1671
How ICA virtual channels work 1671
Graphics virtual channel on the server side 1672
Hosting specialized channels in windows services 1672
Creating your own virtual channel using the Virtual Channel SDK 1674
Creating your own virtual channel using the ICA Client Object SDK 1674
Pass-through functionality of virtual channels 1674
Pass-through functionality of virtual channels between a Citrix Virtual Desktop session and a Citrix Virtual App session 1675
Security and ICA virtual channels 1676
Best practices 1676
See also 1678
Double hop in Citrix DaaS™ 1679
System requirements 1679
Deployment considerations for HDX™ in double hop 1680
Graphics 1680
Latency 1680

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multimedia 1680

USB device redirection 1680

Support exceptions 1681

HDX™ connectivity 1682

Adaptive transport 1682

Configuration 1682

How it works 1683

System requirements 1684

Network requirements 1685

Session hosts 1685

Internal network 1685

Client network 1686

Enlightened Data Transport 1687

Things to know 1688

EDT MTU Discovery 1688

Troubleshooting 1688

When sessions fail to connect with EDT 1690

Known issues 1691

Rendezvous protocol 1691

Rendezvous V1 1692

Requirements 1692

Proxy configuration 1693

Rendezvous validation 1695

Other considerations 1695

Rendezvous V2 1695

Requirements 1696

Proxy configuration 1697

How to configure Rendezvous 1699

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Other considerations 1700
Known Issues 1700
Rendezvous traffic flow 1701
HDX™ Direct 1702
System requirements 1702
Network requirements 1703
Session hosts 1703
Client network 1703
Data center network 1704
Configuration 1705
Considerations 1706
How it works 1706
Internal users 1706
External users 1707
Certificate management 1708
Overview 1708
Session host 1709
Client device 1710
Using custom certificates 1710
NAT Compatibility 1712
Validations 1712
Troubleshooting 1715
When HDX Direct fails to establish a direct connection 1716
Event logs 1718
Known issues 1719
Secure HDX™ 1720
System requirements 1720
Configuration 1721

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX Insight and Smart Control 1721
Considerations 1722
Troubleshooting 1722
When Secure HDX does not get enabled in the session 1723
Network telemetry 1723
System requirements 1723
Network requirements 1724
Session hosts 1724
Internal network 1724
Configuration 1725
Considerations 1725
Virtual channel allow list 1725
Configuration 1726
Adding virtual channels to the allow list 1726
For single processes 1726
For multiple processes 1726
Using wildcards 1727
Using system environment variables 1728
Obtain virtual channel names and processes 1728
Considerations for Citrix virtual channels 1729
Multimedia Redirection 1729
HDX RealTime Optimization Pack for Skype for Business 1729
Considerations for third-party virtual channels 1730
Microsoft Teams 1730
Zoom Meetings for VDI 1730
Troubleshooting 1731
Event logs 1731
Known third-party virtual channels 1734

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual Channel Allow List for DVC 1734
Configuration 1734
Adding dynamic virtual channels to the allow list 1735
Devices 1737
Optimized vs. generic USB device 1737
Mobile and touch screen devices 1738
Requirements 1738
Citrix® control plane 1738
Session host 1738
Client device 1739
Tablet mode for touch-screen devices using Windows Continuum 1739
XenServer® 1739
Session host 1739
Microsoft Surface Pro and Surface Book pens 1740
Citrix control plane 1741
Session host 1741
Client device 1741
Known issues 1741
Serial devices 1742
Map a client COM port to a server COM port 1742
Troubleshoot 1744
Specialty keyboards 1747
Bloomberg keyboards 1747
Webcams 1749
High definition webcam streaming 1749
Scanning 1749
TWAIN Redirection 1750
Introduction 1750

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements 1750
Configuration 1751
Troubleshooting 1752
WIA Devices 1752
Requirements 1752
USB Devices 1753
Configuration 1754
How to configure USB redirection 1754
Composite Devices and Device Splitting 1757
Configuring a signature pad 1758
Configuring Bloomberg keyboard using USB redirection 1759
Configuring a FIDO2 key using USB redirection 1760
Configuring a 3-d mouse using USB redirection 1761
Troubleshooting 1761
Event Logs 1764
USB Diagnostics Tool 1766
Requirements 1767
What does the tool do? 1767
Device List 1770
Legacy USB Redirection Configuration 1771
Enabling Generic USB Redirection 1771
Creating USB Redirection Policy Rules 1772
Configure automatic redirection of USB devices 1773
Graphics 1777
Related information 1778
HDX™ 3D Pro 1779
GPU acceleration for Windows multi-session OS 1780
GPU sharing 1780

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DirectX, Direct3D, and WPF rendering 1781
GPU acceleration for CUDA or OpenCL applications 1782
GPU acceleration for Windows single-session OS 1782
Optimize the HDX 3D Pro user experience 1786
Thinwire 1786
Introduction 1786
HDX™ 3D Pro 1787
Requirements 1787
Encoding methods 1788
Configuration 1788
Monitoring Thinwire 1789
Lossless compression codec (MDRLE) 1791
Progressive Mode 1791
Changing progressive mode behavior 1792
H.264 Build to lossless 1792
Text-based session watermark 1792
Multimedia 1795
Example scenarios 1796
Double hop support with media redirection technologies 1797
Audio 1798
Audio quality 1798
Client audio redirection 1799
Client microphone redirection 1800
Audio Plug N Play 1800
Audio redirection bandwidth limit and audio redirection bandwidth limit percent 1800
Audio over UDP Real-time Transport and Audio UDP port range 1800
Audio setting policies for user devices 1801
Avoid echo during multimedia conferences 1802

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Softphones 1803

Limitation 1807

Browser content redirection 1807

Introduction 1807

How it works 1807

Key Benefits 1808

System Requirements 1809

Server side components 1809

Client side components 1809

Steps to Configure 1811

Configuration Options 1812

Redirection mechanisms 1812

Authentication handling 1814

Use Cases 1816

Extension Deployment 1816

Troubleshooting 1821

Browser Content Redirection Limitations 1821

Server side limitations (VDA) 1821

Client side limitations (CWA) 1822

HDX™ video conferencing and webcam video compression 1822

HDX webcam video compression 1822

HDX webcam video compression requirements 1823

High-definition webcam streaming 1825

HDX plug-n-play generic USB redirection 1825

HTML5 multimedia redirection 1826

HTTP progressive downloads 1826

Comparing HTML5 and Flash 1826

Requirements 1827

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Components of the HTML5 video redirection solution 1828
How do I enable HTML5 video redirection? 1828
Troubleshooting Tips 1829
Optimization for Microsoft Teams (New) 1829
Optimization approaches 1829
Key distinctions 1830
Interoperability and roaming 1830
Citrix HDX™ Optimization 1831
System requirements 1831
Deployment 1832
Networking considerations 1833
Feature matrix and version support 1833
Troubleshooting and other considerations 1836
Known limitations 1836
New VDI solution for Teams 1837
System requirements 1838
Components 1839
Deployment 1839
Options to install the Teams plug-in 1840
Plug-in update scenarios 1842
Teams as a Citrix published app 1843
Interoperability and roaming 1843
Networking considerations 1843
Feature support 1843
Troubleshooting 1843
Known limitations 1844
Optimization for Microsoft Teams (Classic) 1844
Microsoft Teams installation 1845

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For Remote PC Access 1846

For App Layering 1847

Profile Management recommendations 1847

Machine-wide installer 1848

Recommendations 1848

Per-user installer 1849

Best Practices 1849

System requirements 1851

Minimum recommended version - Delivery Controller (DDCs) 1906.2 1851

Minimum version - Virtual Delivery Agents (VDAs) 1906.2 1851

Recommended version – Citrix Workspace app for Windows latest CR and Minimum version - Citrix Workspace app 1907 for Windows 1851

Minimum version - Citrix Workspace app 2006 for Linux 1852

Minimum version - Citrix Workspace app 2012 for Mac 1852

Minimum version - Latest version of Citrix Workspace app for Chrome OS running on the latest version of Chrome OS 1853

Single Server Scalability 1854

Hardware (system under test) 1854

Software 1854

Terminology 1854

How Microsoft Teams is stress-tested 1855

Results 1855

Feature matrix and version support 1856

Enable optimization of Microsoft Teams 1858

Network requirements 1860

Summary of key network recommendations for Real Time Protocol (RTP) traffic 1860

Proxy servers 1862

Call establishment and media flow paths 1863

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Call setup 1865
Microsoft Phone System 1866
DTMF 1866
Support for dynamic e911 1867
Firewall considerations 1868
Microsoft Teams and Skype for Business Coexistence 1869
Citrix SD-WAN™: optimized network connectivity for Microsoft Teams 1869
Multi-window meetings and chat 1870
Background blurring and background effects 1871
Setting a custom background image 1872
Client CPU Consumption considerations 1874
Gallery view and active speakers in Microsoft Teams 1874
Screen sharing in Microsoft Teams 1877
Multimonitor 1878
App sharing 1879
Peripherals in Microsoft Teams 1882
Fallback mode 1883
Known limitations 1885
Citrix limitations 1885
Simulcast 1886
Microsoft limitations 1887
Citrix and Microsoft limitations 1887
Upcoming Microsoft Teams Single-Window EOL 1887
Deprecation announcement of the SDP format (Plan B) from WebRTC 1888
Products that are affected 1888
Replacement for Plan B 1889
Additional information 1889
Monitor, troubleshoot, and support Microsoft Teams 1889

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitor Teams 1889
Troubleshoot 1890
Support 1894
Windows Media redirection 1899
Virtual Channel Plugin Manager 1900
Introduction 1900
System Requirements 1900
Supported applications 1901
Virtual Channel Plugin Manager overview 1901
Understanding the Feature 1901
Virtual Channel Plugin Manager Configuration 1902
Deployment 1902
Procedure 1902
Known Issues & Limitations 1904
Unified Communications SDK Optimization 1904
Introduction 1904
How it works 1905
What’s New 1905
New Features 1906
Key Benefits 1907
Use Cases 1907
UCSDK Architecture 1908
System Requirements 1909
Fully Compatible Versions 1909
Configuration 1910
On the VDA 1910
On the Client 1910
Versions and Feature Matrix 1911

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Current Vendor Support 1913
Troubleshooting 1914
Known Issues & Limitations 1914
General content redirection 1915
Client folder redirection 1915
Bidirectional content redirection configuration 1917
Host-to-client redirection 1919
System requirements 1920
Configuration 1920
Server VDA default browser configuration 1923
Bidirectional content redirection 1924
System requirements 1924
Configuration 1924
Wildcard redirection from Citrix VDA to client 1925
Custom protocol redirection from VDA to client 1926
Other considerations 1926
Local app access and URL redirection 1927
Introduction 1927
Requirements, considerations, and limitations 1929
Interaction with Windows 1930
Configure Local App Access and URL redirection 1931
Enable Local App Access and URL redirection 1931
Enable the Local App Access template using the Group Policy editor 1933
Provide access only to published applications 1933
Register browser add-ons 1935
URL interception across browsers 1935
Configure local application behavior on logoff and disconnect 1936
Generic USB redirection and client drive considerations 1936

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Performance considerations for USB devices 1937
Security considerations for USB devices 1938
Compatibility with generic USB redirection 1938
Configure generic USB redirection 1939
Enable generic USB redirection 1940
Configuring the types of USB devices available for generic USB redirection 1942
Use and remove USB devices 1946
Security controls for USB mass storage devices 1946
Manage 1948
Adaptive access 1949
Device Posture service 1949
Adaptive Authentication service 1950
Adaptive access based on user's network location 1950
Entitlements 1951
Prerequisites 1951
Points to note 1952
Enable the Adaptive Access feature 1953
Configure adaptive access 1955
Network location tags 1961
Known issues 1963
Configure session recording policies based on tags 1963
Applications 1963
Introduction 1963
Add applications 1964
Add one or more applications to multiple delivery groups or application groups 1964
Add one or more applications to a delivery group or application group 1964
Select groups 1965
Specify applications 1965

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change an application's group association 1967

Change application properties 1968

Configure application limits 1970

Duplicate, enable or disable, rename, or delete an application 1973

Remove applications from a delivery group 1974

Remove applications from an application group 1974

Pass parameters to published applications 1974

Troubleshooting session sign-out issues with Published Applications 1975

Step 2: Identifying for those published applications if they produce any additional (child) processes 1976

Step 3: Add these processes to a specified registry entry to prevent them from holding up sign-out 1976

Step-by-step troubleshooting guide 1977

How to modify LogonUI to view Windows disclaimer message in full size when opening published applications 1984

Disable a tilebar 1984

Manage application folders 1985

Control local launch of applications on published desktops 1987

App packages 1988

App-V applications 1988

MSIX and MSIX app attach applications 1992

FlexApp applications 1993

Elastic App applications 1993

Cloudpaging applications 1994

Deploy and deliver app packages 1995

Best practices 2006

Advanced 2007

Migrate from App-V full infrastructure to Single Admin workflow 2009

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot App-V applications (Single Admin model) 2011
Autoscale™ 2016
Typical use cases 2016
Supported VDA hosting platforms 2017
Supported workloads 2017
Benefits 2017
Watch a 2-minute video 2017
Get started with Autoscale™ 2018
Basic concepts 2018
Enable Autoscale for a delivery group 2025
Autoscale options for VMs with user sessions 2027
Monitor metrics 2029
Autoscale on hibernated VMs 2029
More information 2030
Schedule-based and load-based settings 2030
How Autoscale™ power manages machines 2030
User interfaces 2031
Schedule-based settings 2036
Load-based settings 2039
Miscellaneous settings 2040
How capacity buffer works 2043
Multi-session OS delivery groups 2044
Single-session OS random delivery groups 2048
Single-session OS static delivery groups 2053
Dynamic session timeouts 2057
FAQ 2060
Autoscaling tagged machines (cloud burst) 2060
Introduction 2060

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use Studio to autoscale certain tagged machines 2061
Use PowerShell to autoscale certain tagged machines 2066
Example scenario 2067
Dynamic machine provisioning 2070
Download the script 2071
How the script works 2071
Prerequisites 2074
Permissions, recommendations, and notices 2074
Authentication API 2075
Create an automated task using Windows Task Scheduler 2075
Script execution example 2076
Troubleshooting checklist for the script 2076
Autoscale™ plug-in 2077
Autoscale holiday plug-in 2077
Intelligent Autoscale schedules plug-in 2080
User logoff notifications 2083
Notify and force user logoff 2084
Send logoff reminders without forcing user logoff 2085
Neither notify nor force user logoff 2087
Considerations 2087
Analyze the effectiveness of Autoscale™ settings 2087
Broker PowerShell SDK commands 2090
Set-BrokerDesktopGroup 2090
New-BrokerPowerTimeScheme 2092
Parameters for dynamic session timeouts 2093
Cloud Health Check 2094
Installation 2095
Permissions and requirements 2096

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About health checks 2097
VDA health checks 2097
StoreFront health checks 2098
Running Cloud Health Check 2099
Import VDA machines 2101
Retrieve VDA machines 2107
Heath check results 2111
Running Cloud Health Check on the command line 2111
Command-line arguments 2112
Exit codes 2113
Reports 2113
Updating Cloud Health Check 2114
Cloud Health Check scheduler 2115
Set up the schedule 2115
View schedule results 2120
Disable schedules 2123
More information 2124
Verification tests 2124
Usage data collection 2125
Automatic fix 2126
Result report 2127
Troubleshooting 2128
Feedback 2128
Configuration logging 2129
Update the retention of DaaS configuration logs 2129
What is logged 2130
View configuration log content 2131
View tasks related to machine catalog operations 2132

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View API logs 2133
View PowerShell logs 2134
Associate metadata with configuration logs 2134
Set the metadata 2134
Retrieve using the metadata 2135
Remove the metadata 2135
Generate reports 2136
Schedule periodic data deletion 2136
Differences from on-premises Citrix Virtual Apps and Desktops 2136
Delegated administration 2137
Overview 2137
Administrators, roles, and scopes 2137
Built-in roles and scopes 2138
How many administrators you need 2141
Administrator management summary 2141
Add an administrator 2142
Create and manage roles 2143
Create and manage scopes 2146
Create scopes 2146
Manage scopes 2149
Manage tenants 2149
Configure custom access for an administrator 2152
Differences from on-premises Citrix Virtual Apps and Desktops 2155
More information 2156
Home page 2156
Resources 2157
Sessions 2158
Recommendations 2158

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- What's new 2159
- Preview features 2159
- Configuration guides 2159
- Errors and warnings 2160
- Advisor 2160
- Customize the Home page 2161

Licenses 2161

- Configure a Microsoft RDS License Server for Windows Server workloads 2161
- Citrix license usage 2162

Local Host Cache 2162

- Overview 2162
- How it works 2163
  - During normal brokering operation 2163
  - When LHC mode becomes active 2164
  - Zones with multiple Cloud Connectors 2165
- Local Host Cache data content 2166
- Local Host Cache states 2166
- Important considerations during LHC mode 2168
  - Application and desktop support 2170
  - StoreFront configuration 2173
- Validate Local Host Cache working 2173
- Monitor Local Host Cache 2174
  - Event logs 2174
- Citrix Monitor 2177
- Force Local Host Cache mode 2177
- Troubleshoot synchronization import failures 2178
  - Local Host Cache PowerShell commands 2179
- More information 2181

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Local Host Cache Visibility Tool 2182

Overview 2182

Prerequisites 2182

Get started 2183

Troubleshooting 2196

Best practices 2198

Examples 2199

Advanced scenarios 2202

Log server settings 2204

Machines and sessions (Search > Default view) 2205

Learn about the default view 2205

Search for instances 2209

Search using filters 2209

Save the current filter set for a quick search 2210

Pin a filter field in the search bar 2210

Search using the quick search box 2211

Tips to enhance a search 2211

Customize columns to display 2212

Manage machines and sessions 2213

Good to know 2213

Perform actions on machines or sessions 2213

Export machine or session data to CSV files 2214

Machine actions and columns 2214

Actions 2214

Columns 2217

Session actions and columns 2232

Actions 2233

Columns 2234

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitor MCS-provisioned machines in **Search > Hardware view** 2239
Learn about the hardware view 2240
Reference: Machine columns 2242
Multi-site management and user resource aggregation 2243
Overview 2244
Administrator roles and permissions 2244
Limitations 2245
Best practices for multi-site management 2245
Full access administrators: Set up centralized site management 2246
Preparation 2246
Set up centralized site management 2246
Add or remove a secondary site 2249
Administrators: Manage sites from a single interface 2250
Considerations when switching between sites 2250
Manage sites 2251
Administrators: Monitor sites from a single interface 2251
Typical use cases 2251
Efficient site administration 2252
Mergers and acquisitions 2252
End-User resource aggregation 2252
Manage personal preferences in Studio 2253
Security keys 2254
Configure settings for your deployment 2254
Use Studio 2254
Use the Remote PowerShell SDK 2256
Configure settings in StoreFront 2257
Configure settings in Citrix ADC 2258
Configuration changes if the Citrix ADC appliance is already configured with Citrix Daas 2268

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session resilience settings 2270
Session reliability 2270
Auto Client Reconnect 2272
ICA Keep-Alive 2273
Workspace control 2274
Session roaming 2276
Configure session roaming 2276
Logon interval 2277
Tags 2278
Introduction 2278
Tag restrictions for a desktop or an application group 2279
Example 1: Simple layout 2280
Example 2: More complex layout 2280
Manage tags and tag restrictions 2281
Use the Manage Tags feature 2282
Manage tag restrictions 2285
Cautions when working with tags 2285
How to configure example 2 2286
Apply tags to machine catalogs 2287
Use PowerShell to apply tags to catalogs 2288
Auto tags 2288
Use cases 2288
PowerShell commands 2289
More information 2290
Tasks in Task Center 2290
Access Task Center 2290
View and manage recent tasks 2291
View and manage recurring tasks 2292

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported task types 2292
Citrix Troubleshoot Connection 2292
Overview 2293
Connection paths analyzed 2293
Enhanced error messages and diagnostics 2293
Self-recovery and remediation actions 2293
System requirements 2294
How to use 2294
Important considerations 2294
Error codes 2294
Common server-side errors 2294
Citrix Workspace app for Windows 2296
Citrix Workspace app for Mac 2298
Citrix Workspace app for iOS 2299
Citrix Workspace app for Android 2301
Troubleshoot VDA registration and session launch issues 2302
Prerequisites 2302
Run health checks for VDAs 2303
User access 2305
Using Citrix® StoreFront Cloud 2305
Service continuity 2305
Using on-premises StoreFront 2306
End user access 2306
Remote access using Citrix Gateway 2306
Local Host Cache 2306
Virtual IP and virtual loopback 2307
Virtual IP 2308
How Microsoft Remote Desktop (RD) IP virtualization works 2308

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual loopback 2309
Related feature 2310
Zones 2310
Introduction 2310
Differences from zones in on-premises Citrix Virtual Apps and Desktops environments 2311
What's in a zone 2311
Where VDAs register 2312
Zone preference 2313
How zone preference works 2313
Tailoring zone preference 2315
How preferred zones affect session use 2315
Other zone preference considerations 2316
Permissions to manage zones 2317
Zone creation 2317
Add or change a zone description 2317
Assign scopes to a zone 2317
Move resources from one zone to another zone 2318
Zone deletion 2318
Add a home zone for a user 2318
Remove a home zone for a user 2319
Manage home zones for applications 2319
Other actions that include specifying zones 2320
Troubleshooting 2320
Remove broker user from the cache 2324
Monitor 2326
Site analytics 2328
Monitor sessions 2330
Disable the visibility of running applications in the Activity Manager 2332

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access Citrix Analytics for Performance™ - Session Details 2332
Session transport protocol 2333
Export reports 2335
Supported export limits 2335
Error Handling 2336
Monitor hotfixes 2336
Control user machine power states 2336
Prevent connections to machines 2337
Application Analytics 2338
Alerts and notifications 2338
Citrix® alerts 2340
Smart alert policies 2340
Advanced alert policies 2341
Create alerts policies 2356
Alerts policies conditions 2362
Configure alerts policies with webhooks 2368
Bulk alert dismissal 2373
Webhook configuration using PowerShell SDK 2373
Local Host Cache config sync failure alert monitoring 2379
Hypervisor Alerts Monitoring 2379
Thresholds 2382
Prerequisites 2383
Predefined thresholds 2383
Custom thresholds 2385
Manage thresholds 2385
Troubleshooting 2387
Application usage monitoring 2387
Least used and not used apps report 2389

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filter data to troubleshoot failures 2392
Unified Communication app metrics 2395
Monitor historical trends across a site 2396
Available trends 2397
Monitor Autoscale-managed machines 2403
Machine Usage 2403
Estimated Savings 2404
Alert notifications for machines and sessions 2405
Machine status 2406
Load Evaluation trends 2406
Troubleshoot deployments 2406
Troubleshoot applications 2407
Application Analytics 2407
Real-time application monitoring 2408
Historical application failure monitoring 2409
Application probing 2411
Desktop probing 2416
Machine health monitoring 2421
1. Introduction: What's New? 2421
2. Understanding the New Visualizations 2422
3. Enhanced Tabular Data 2424
4. Support for new Time Range Filters 2426
VDA Health Monitoring Metrics: Supported platforms and versions 2426
Troubleshoot user issues 2427
Microsoft Teams optimization status 2428
Troubleshooting tips 2430
Session Performance 2431
Search tips 2431

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diagnose conditional authentication failures 2431
Diagnose Device Posture service transactions 2433
Diagnose session startup issues 2441
Diagnose user logon issues 2446
Diagnose session performance issues 2455
Diagnose application performance issues 2486
Diagnose historical user sessions 2496
Shadow users 2499
Send messages to users 2503
Custom role to limit bulk action option for user actions 2504
Resolve application failures 2505
Restore desktop connections 2506
Restore sessions 2507
Run HDX™ channel system reports 2508
Reset a user profile 2508
Record sessions 2511
Troubleshoot machines 2514
Infrastructure monitoring 2528
Key features 2529
Use-cases 2529
Prerequisites 2530
Getting started with Infrastructure Monitoring 2531
Step 1: Installation of Citrix Infrastructure Monitor 2531
Step 2: Register Citrix Infrastructure Monitor 2534
Steps to Configure HTTPS for Citrix Infrastructure Monitor 2538
Set up Remote PowerShell SDK 2546
Prerequisites 2546
Setting up of Remote PowerShell SDK 2546

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage connections 2547
View connections 2547
Edit the connection 2549
Remove a component 2549
Infrastructure dashboard 2550
Provisioning Service health metrics 2550
StoreFront™ health metrics 2554
Cloud Connector health metrics 2558
Connector Appliance health metrics 2564
Create and manage alerts 2568
Application and Desktop Probing 2569
Requirements 2569
Configuration 2570
Step 1: Install and configure the Citrix Probe Agent 2571
Step 2: Configure Probing in Monitor 2574
Step 3: Probe execution 2575
Step 4: View probe results 2576
Cost optimization 2577
How is the cost calculated for cost optimization 2578
Cost for Azure machines 2578
Calculating costs for machines other than Azure 2580
Export data 2580
Setup data integration 2581
ODATA queries for cost optimization 2581
Cost savings 2583
Workload rightsizing 2591
Usage analysis 2592
Sizing analysis 2594

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Best practices 2596
Key terms and charts 2596
Cost summary 2597
Cost modeling 2601
Types of plans 2602
Power management strategies 2604
Machine consumption and recommendations 2605
Analyze per virtual machine series 2605
Feature compatibility matrix 2606
Aggregated Search across multiple DaaS instances 2618
Pre-requisites 2618
How it works 2618
Delegated administration 2619
Integrations and data exports 2623
View available integrations 2624
Reporting and dashboards 2624
Integrations with alerting and ITSM tools 2624
Integration with Webhook 2625
Integrating the Webhook Profiles with Citrix Alerts 2626
View supported developer tools 2626
Kafka Data Exports 2627
Monitor service API 2630
Webhook 2630
Microsoft Sentinel integration 2631
Prerequisites 2631
Install the Citrix SPA Sentinel App 2632
Configure Logstash 2634
Select SPA and DPS event types 2635

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verify data ingestion 2636
View workbook 2636
Secure Private Access 2637
Secure Private Access tab on Monitor 2638
Key benefits 2638
Requirements 2638
Visibility for Secure Private Access Service 2639
Monitor and troubleshoot Secure Private Access 2641
Service entitlements 2641
Supported clients 2641
How to access Monitor 2641
Session definitions 2641
View a Secure Private Access session by user 2643
Activity Manager for Secure Private Access session 2645
Secure Private Access Session Details page 2647
Sample topology diagrams for the various apps 2659
Create and manage alerts 2666
Support for Chrome Enterprise Premium 2666
Observability for multi-session VDA 2668
Troubleshoot application reachability (Connector Appliance to backend app) 2669
Requirements 2670
Probe protocols and inputs 2670
Run a probe from the Infrastructure view 2671
Run a probe from the Application Topology view 2673
Understand the probe results 2676
Successful probe 2676
Probe through a proxy 2677
Failed probe 2677

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Considerations 2678
Data granularity and retention 2678
Aggregation of data values 2678
Concurrent data evaluation 2679
Correlation of summary tables with raw data 2679
Granularity and retention 2680
Session launch diagnostics 2688
Prerequisites 2688
Steps to diagnose session launch failure 2689
Components 2691
Error details 2692
Transaction Logs 2693
Error code 2693
Broker agent 2693
bka.hdx.validate.failure.ticket_not_found 2693
Broker 2694
HDX VDA Linux 2696
HDX VDA Windows 2699
MCS 2703
Profile Management 2706
WEM Agent 2706
Android Postlaunch 2706
Android Prelaunch 2708
Linux Postlaunch 2711
Linux Prelaunch 2713
Mac Postlaunch 2714
Mac Prelaunch 2716
Windows Postlaunch 2717

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows Prelaunch 2719

Workspace 2721

Citrix Gateway as a service 2727

XAXD proxy 2731

Real time communications dashboard 2735

Microsoft Teams 2735

Prerequisites 2735

Getting started 2736

Connection to Microsoft Graph API 2736

Microsoft Teams dashboard 2741

Service continuity monitoring dashboard 2743

Overview 2743

What is an instance, and how is data collected from it? 2743

How readiness is calculated 2743

For native app launch 2743

For hybrid launch (login from web, session launch via CWA app) 2744

Version requirements 2744

Dashboard features 2744

Instance readiness over time chart 2744

Day-wise overview panel and instance charts 2745

Filters 2746

Table fields 2746

Logs 2748

Prerequisites and Configuration 2749

Getting Started 2749

Accessing the Logs View 2749

Using the Logs View 2749

Insights 2750

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Black hole machines 2751
Zombie Sessions 2753
Overloaded Machines 2754
Connection failures 2754
Filter View 2756
Alerts 2757
Managing Default Policies 2758
Creating Custom Policies 2758
Alert notifications 2758
Alert for Black Hole Machines 2759
Alert for Machines with Zombie Sessions 2760
Alert for Overloaded Machines 2760
Re-alerts 2761
Geo Map visualization 2761
Overview 2761
Prerequisites 2762
VDAs 2762
Key benefits 2762
User interface components 2763
Navigation and view options 2763
Summary dashboard metrics 2764
Performance classification 2764
Map legend and threshold controls 2765
System requirements and notifications 2765
Citrix Workspace app version compatibility 2765
Configuration options 2766
Setting performance thresholds 2766
Time range configuration 2766

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Map view usage 2766
Regional performance troubleshooting 2766
Capacity planning 2766
Global deployment assessment 2767
Threshold optimization 2767
Troubleshooting 2767
Missing geographical data 2767
Performance categorization issues 2767
Data refresh issues 2767
Best practices 2768
deviceTRUST® integration in Monitor 2768
Highlighted session interruptions on the User Details page 2768
View deviceTRUST issues button on the User Details page 2769
Detailed deviceTRUST failure information 2769
Updated Denied Access tab 2770
Session Score 2770
Prerequisites 2770
Overview 2771
Endpoint OS Version Visibility 2772
Advantages 2772
Example usage 2772
Applicability 2773
System requirements 2773
Limitations 2773
Endpoint Security Policy activation & threat detection reporting 2774
Advisor 2776
Benefits 2776
Check for recommendations 2777

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filter recommendations 2778
Review and act on recommendations 2779
View recommendation details 2779
Implement recommended actions 2780
Dismiss recommendations 2781
Dismiss specific affected targets in a recommendation 2781
Customize check rules 2782
View the full site check report 2783
Set up StoreFront for Advisor check 2783
References 2784
Security recommendations 2784
Reliability recommendations 2793
Performance recommendations 2804
Operational excellence recommendations 2812
Cost optimization recommendations 2818
VDA Upgrade Service (VUS) 2820
Prerequisites for upgrading VDAs using VUS 2820
Enable the VDA Upgrade Service 2821
VDA Requirements 2822
VDA Version 2822
Source VDA operating system 2822
Provisioning Type 2822
VDA Upgrade Agent 2822
Permissions 2823
VDA State 2823
Connectivity 2824
VDAs with Proxy configurations 2825
VDAs installed using the VDAWorkstationCoreSetup.exe 2826

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Government Cloud prerequisites for VDA upgrades (VUS) 2826
Pre-requisites 2826
Required outbound endpoint access 2826
Why these endpoints are required 2827
Government storage and KeyVault pre-requisites 2827
FedRAMP boundary considerations 2827
Pre-upgrade verification checklist 2827
Upgrade VDAs using VUS 2828
Scheduling Upgrades 2828
Considerations 2828
Restrict upgrades to tagged machines 2828
Key Differences 2829
How scheduled upgrades work 2831
VDA Versions Available 2832
Additional Components 2833
Features 2834
Concurrency 2835
Failure Threshold 2835
VDA Installer Location 2836
Force Logoff Sessions 2838
Restart VDAs before starting the upgrade 2839
Power on machines to upgrade VDA 2839
Edit or Cancel the VDA workflow 2841
Monitor and Troubleshoot VUS 2841
Monitoring Scheduled VDA Upgrades 2841
VDA Upgrade 2841
VDA Upgrade State 2843
Troubleshooting Scheduled VDA Upgrades 2845

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA Installation Logs 2845
VDA Upgrade Agent Version 2846
Logs related to the VDA Upgrade Agent 2846
Troubleshoot VDA upgrade download failures 2848
Troubleshoot VDA upgrade validation failures 2849
Citrix DaaS™ for Citrix Service Providers 2850
Requirements 2850
Limitations 2850
Partner service administration 2851
Step 1: Add a customer 2851
Step 2: Add Citrix® multitenant DaaS to a customer 2852
Step 3: Set up a resource location 2854
Step 4: Federate domains 2854
Add a customer to a domain 2854
Remove a customer from a domain 2855
Step 5: Assign a zone to tenant scope 2856
Step 6: Create a policy set for tenant scope 2856
Step 7: Set up catalogs and groups to deliver apps and desktops 2857
Step 8: Control administrator access to customers 2858
Add a partner administrator with restricted access 2858
Edit delegated administration permissions for administrators 2858
View DaaS administrators and their assigned roles and scopes 2859
Export administrator activities for auditing 2859
Step 9: Configure stores 2860
Monitor a customer's service 2861
Remove the DaaS service from a customer 2862
Tenant service administration 2863
Add tenant administrators 2863

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access the Studio console in the tenant account 2864
Update host connections 2865
Create catalogs and delivery groups 2865
Manage policies in the tenant account 2866
Citrix Gateway 2867
SDKs and APIs 2868
Citrix DaaS™ Remote PowerShell SDK 2868
How this SDK differs from the SDK for customer-managed deployments 2868
Prerequisites 2869
Commercial 2869
Japan 2869
Government 2869
Install and use the Remote PowerShell SDK 2869
Use the Remote PowerShell SDK with a proxy 2870
Example activities 2871
Support and limitations 2873
Citrix DaaS discovery module for App-V packages and servers 2880
Add App-V packages to the Application Library in Citrix Cloud 2881
High-level PowerShell functions 2882
Example activities 2883
Limitations 2884
Monitor Service OData API 2884
Citrix DaaS APIs 2885
Disclaimer 2885
Citrix DaaS™ document history 2886

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overview

Introduction

Citrix DaaS™ is a service that provides app and desktop virtualization, giving IT control of on-prem or cloud-hosted virtual machines, applications, and security while providing anywhere access for any device. End users can use applications and desktops independently of the device's operating system and interface.

Using Citrix DaaS, you can deliver secure virtual apps and desktops to any device, leaving most of the installation, setup, and upgrades to Citrix. You maintain complete control over applications, policies, and users while delivering the best user experience on any device.

Citrix DaaS allows you to manage on-premises data center and public cloud workloads together in a hybrid deployment. You can connect to public clouds Microsoft Azure, Amazon Web Services (AWS), and Google Cloud, plus on-premises hypervisors such as XenServer®, Microsoft Hyper-V, Nutanix AHV, and VMware vSphere. The hybrid, multi-cloud approach gives you the flexibility to deploy different applications in different resource locations worldwide.

Citrix DaaS offers several ways to deliver apps and desktops.

- Delivery methods describes the primary ways, with use-cases and pros/cons.
- Delivery models lists more choices, and also offers VDI model comparisons.

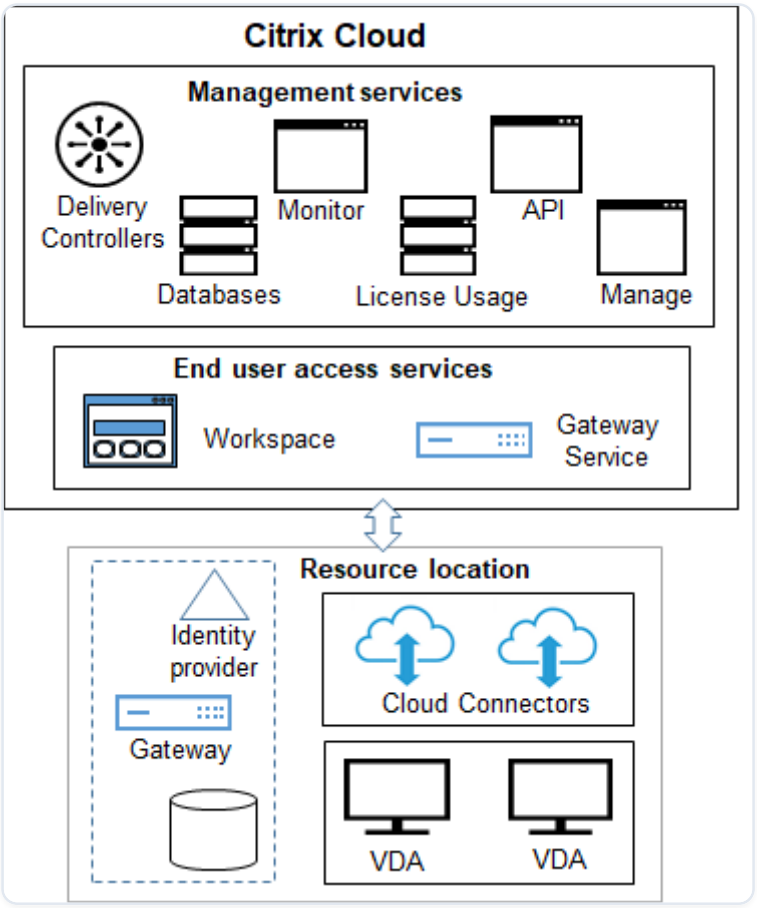
Citrix Managed Azure further simplifies the deployment of virtual apps and desktops. With Citrix Managed Azure, Citrix also manages the hosting of Azure workloads.

Learn more about the advantages of using this service.

Site overview

The following graphic shows the services and components that Citrix administrators work with in a Citrix DaaS production deployment (also known as a site).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



As shown in the graphic, Citrix manages the user access and management services and components in Citrix Cloud. The applications and desktops that you deliver to users reside on machines in one or more resource locations. In a Citrix DaaS deployment, a resource location contains components from the access layer and resource layers. Each resource location is considered a zone.

If you recently migrated from Citrix Virtual Apps and Desktops™, you'll see that Citrix DaaS eliminates most of the component setup work required in an on-premises deployment.

Components and services managed by Citrix

- **Delivery Controllers:** Citrix DaaS provides the functionality to load balance applications and desktops, authenticate users, and broker or prioritize connections directly from the cloud, without the need to manage Delivery Controllers, as with Citrix Virtual Apps and Desktops.
- **Databases:** Site configuration, monitoring, and configuration logging data is stored by the cloud service, eliminating the SQL database requirement of the on-premises Citrix Virtual Apps and Desktops product.
- **Licensing:** Manages licenses and provides usage statistics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Studio:** A web-based, central console that lets you configure, manage, and monitor your DaaS deployments for delivering virtual apps and desktops. For more information, see Plan and build a deployment and Manage your deployments.

  You can also use service APIs and PowerShell commands to configure and manage your DaaS deployments.

- **Monitor:** The Monitor console enables IT support and help desk teams to monitor an environment, troubleshoot issues before they become critical, and perform support tasks for end users. Displays include:

  - Real-time session data from the Broker Service in the Controller, which includes data from the broker agent in the Virtual Deliver Agent (VDA).
  - Historical data from the Monitor Service in the Controller.
  - Data about HDX™ traffic (also known as ICA traffic).

- **Cloud Connectors:** A Cloud Connector is the communications channel between the components in the Citrix Cloud and components in the resource location. In the resource location, the Cloud Connector acts as a proxy for the Delivery Controller™ in Citrix Cloud.

  Every resource location contains at least one Cloud Connector. Two or more Cloud Connectors are recommended for redundancy.

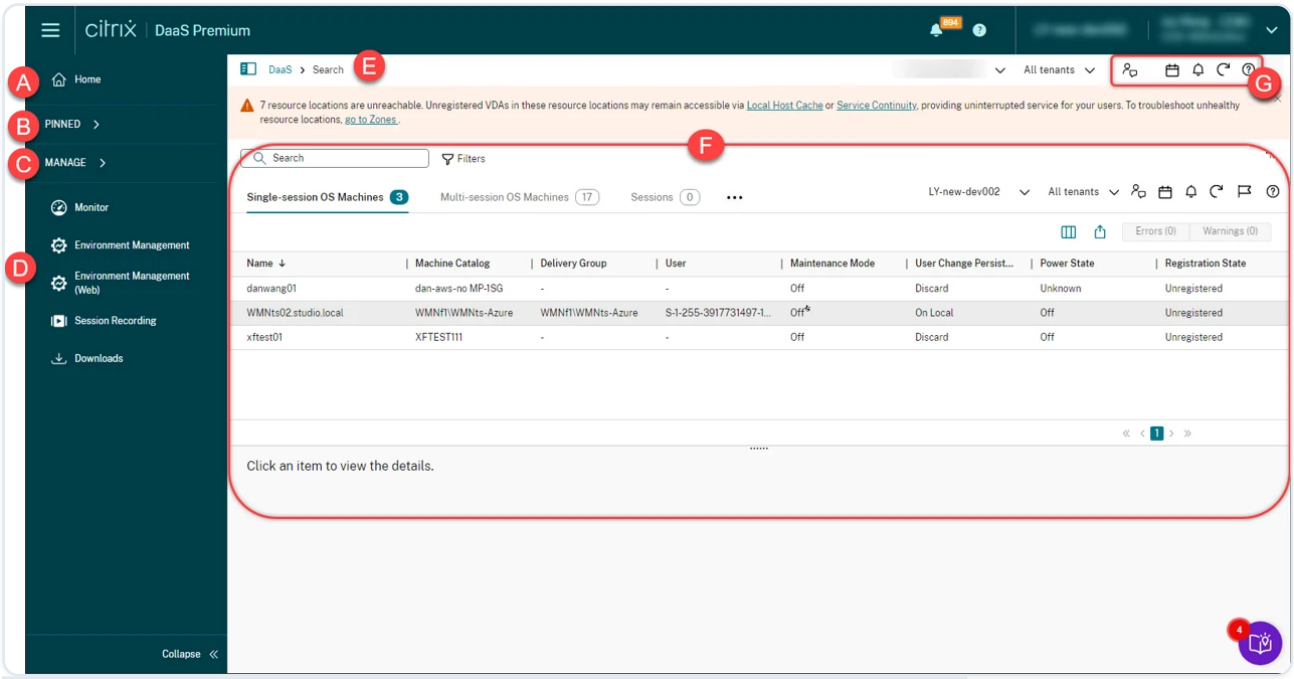
  - When using Studio to provision machines, you first install Cloud Connectors from the Citrix Cloud™ console. For details, see Cloud Connectors.
  - When using Quick Deploy to provision Azure machines, Citrix creates the resource location and Cloud Connectors for you when you create a catalog.

  After Cloud Connectors are installed, Citrix manages and updates them. The only tasks handled by the customer are Cloud Connector Windows updates and patching.

Studio

Studio is a web-based, central portal that lets you configure, manage, and monitor your DaaS deployments for delivering virtual apps and desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



CALLOUT	AREA	DESCRIPTION
A	Home	Provides an overview of your Citrix DaaS deployment and workloads along with information that helps you get the most from your subscription. For more information, see the Home page.
B	PINNED	Visible only after you pin a node in the left pane. Lists nodes that you've pinned.
C	MANAGE	• Full Configuration-related nodes: Let you configure and manage your DaaS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CALLOUT	AREA	DESCRIPTION
		deployments for delivering virtual apps and desktops. Examples include: Search, Machine Catalogs, Delivery Groups, and more. For more information, see Plan and build a deployment and Manage deployments. • Quick Deploy node: Lets you quickly configure and manage your DaaS deployments hosted by other cloud service providers using a guided workflow. Choose from four hosting providers: Microsoft Azure, Microsoft Windows 365, Amazon

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CALLOUT	AREA	DESCRIPTION
		WorkSpace Core, and Google Cloud.
D	Others	• Monitor node: Directs you to the Monitor interface. For more information, see Monitor. • Service nodes: Directs you to the interfaces of value-added services, such as Workspace Environment Management (web) service and Session Recording service. • Downloads node: Directs you to the Downloads page, where you can download software to set up and manage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CALLOUT	AREA	DESCRIPTION
		your DaaS resources.
E	Breadcrumb trail	Provides context and enables quick navigation back to higher-level pages.
F	Working pane	Displays actions and details of a selected node.
G	Common actions	Displays common actions such as Submit feedback, customize the Home page, access the Notification Center, and more. • Notification Center provides real-time updates and a 48-hour history of long-running operations. While an operation is running, a status notification appears below the common actions area to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CALLOUT	AREA	DESCRIPTION	
		indicate its progress.	
		• Task Center displays a comprehensive list of all tasks, organized by category. The UI provides Filter, Search, and other controls consistent with the main view. You can perform actions on any listed task, including common actions like **Delete** and **View details**, and task-specific actions such as Rerun task and Export sub-task status.	

Components and technologies managed by the customer

- **Citrix Gateway:** When users connect from outside the corporate firewall, Citrix DaaS can use Citrix Gateway technology to secure these connections with TLS. The Citrix Gateway or VPX virtual appliance is an SSL VPN appliance deployed in the DMZ. It provides a single secure point of access through the corporate firewall.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix installs and manages the Citrix Gateway service in Citrix Cloud. You can also optionally install Citrix Gateway in resource locations.

- **Active Directory:** Active Directory is used for authentication and authorization. It authenticates users and ensures that they are getting access to appropriate resources. A subscriber's identity defines the services to which they have access in Citrix Cloud. This identity comes from Active Directory domain accounts provided from the domains within the resource location.
- **Identity Provider (IdP):** The IdP is the final authority for the user's identity. Supported IdPs include: on-premises Active Directory, Active Directory plus token, Microsoft Entra ID, Citrix Gateway, and Okta. For more information, see:
  - Tech Brief: Workspace Identity
  - Identity and access management
- **Virtual Delivery Agents (VDAs):** Each physical or virtual machine that delivers resources (applications and desktops) must have a Citrix VDA installed on it. VDAs establish and manage the connection between the machine on which it's installed and the user device, and apply policies that are configured for the session.

  The VDA registers with a Delivery Controller, using a Cloud Connector in the resource location as a proxy.

  Several VDA types are available:

  - VDAs for Windows multi-session operating systems allow multiple users to connect to the machine at one time. This VDA type is usually installed on Windows servers.
  - VDAs for Windows single-session operating systems allow one user to connect to a machine at a time. This VDA type is usually used for VDI.

    A core version of this VDA type is available for use with the Remote PC Access feature. It contains a subset of the features in the full single-session VDA.
  - Linux VDAs support virtual apps and desktops based on an RHEL, CentOS, SUSE, or Ubuntu distribution.

  Throughout this service's documentation, "VDA" often refers to the agent and the machine on which it is installed.
- **Hypervisors and cloud services:** In most production sites, the app and desktop instances (workloads) that you make available (publish) to your users are "hosted" by a supported

© 1997–2026 Citrix Systems, Inc. All rights reserved.

hypervisor or cloud service. (The Remote PC Access feature is usually used with physical machines. Therefore, it does not use hypervisors or cloud services for machine provisioning.)

  - When using Studio, you first create a connection to a supported host hypervisor or cloud service. Next, you use an image (created through that host) to create a catalog of machines that contain the app and desktop instances. Finally, you create a delivery group. Citrix provides various tools to simplify and facilitate how these session hosts are built and maintained.
  - When using Quick Deploy to deliver Azure workloads, you only need to create the catalog. Although you can use your own Azure subscription when creating the catalog, using a Citrix Managed Azure subscription eliminates your need to manage the host, too.

  The app and desktop instances that you publish can be on-premises, hosted in public clouds, or in a hybrid mixture of both.

- **Citrix StoreFront™:** Citrix StoreFront is the customer hosted access tier, as an alternative to Citrix® StoreFront Cloud. For more information, see StoreFront and Citrix® StoreFront Cloud).

Objects you configure to deliver desktops and applications

You configure the following items to deliver apps and desktops in a production environment.

- **Host connection:** A host connection (mentioned earlier) helps enable communication between components in the control plane (Citrix Cloud) and VDAs in a resource location. Connection specifications include:

  - The address and credentials to access the host
  - The storage method to use, and the machines to use for storage
  - Which network the VMs can use

  Remember: When using Quick Deploy, you don't have to create a connection. And if you use Citrix Managed Azure, Citrix manages the hosting, as well.

- **Catalog:** In the Studio and Monitor interfaces, catalogs are called "machine catalogs." A catalog is a collection of virtual or physical machines that have the same operating system type (for example, Windows multi-session, Ubuntu single-session).

  When creating a catalog, you usually use an image, which is also known as a template. (Remote PC Access catalogs usually contain physical machines, so no image is needed.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - When using Quick Deploy, Citrix provides several Citrix prepared images you can use to create your own customized images. Or, you can import images from your own Azure subscription.
  - When using Studio to create VMs using a supported host type, the image usually must be created and reside on a host machine. When creating the catalog, you provide the path to that image.

  Regardless of where the image resides, you can install applications on the image, if you want those apps on all machines created from that image (and don't want to virtualize those apps).

  After the image is ready, you create the catalog.

  - For VMs, MCS creates the machines and the catalog.
  - For Remote PC Access, MCS simply creates the catalog, because the physical machines already exist.

  For more information about MCS, see Image management.

- **Delivery group:** A delivery group specifies:

  - One or more machines from a catalog.
  - Users who are allowed to access those machines.
  - The applications and desktops that users can access through their store.

  When using Quick Deploy, a delivery group is created automatically. (It appears only in the Studio interface.)

- **Application group:** Application groups let you manage collections of applications. You can create application groups for applications shared across different delivery groups or used by a subset of users within delivery groups. Application groups are optional.

Citrix Managed Azure

Citrix Managed Azure is an option available in several Citrix DaaS editions. Using Citrix Managed Azure simplifies the deployment of virtual apps and desktops from Azure. Citrix manages the infrastructure for hosting Azure workloads.

With Citrix Managed Azure, you get a dedicated Citrix-managed Azure subscription and resource location. In that Azure subscription, you create a catalog of VMs. You can:

- Deploy single-session and multi-session Windows OS machines or Linux OS machines, from various supported versions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Choose from a curated list of compute types and storage options in select regions.
- Provision persistent or non-persistent workloads on those machines.
- Choose from several Citrix provided images that have the latest VDA installed. Then, from the Citrix interface, you build your own image from that template, and customize it. You can also import and use images from your own Azure subscriptions.

Even though Citrix manages Azure capacity, if you want to communicate with existing resources on your own Azure subscription, you can use Azure VNet peering to connect resources. You can also use Azure VPN gateway to connect to your on-premises resources directly.

For information about security and responsibilities when using Citrix Managed Azure, see Technical security overview for Citrix Managed Azure.

Ordering Citrix Managed Azure

To get a Citrix Managed Azure subscription, you must subscribe to a supported Citrix service offering, and then order Citrix Managed Azure Consumption Funds. You can order Citrix DaaS and consumption funds through Citrix or from Azure Marketplace. Citrix Managed Azure is supported on the following service offerings:

- Citrix DaaS, Advanced, Advanced Plus, and Premium editions
- Citrix DaaS Standard for Azure edition

For details, see Sign up for Citrix DaaS.

Citrix Managed Azure benefits summary

Using Citrix Managed Azure offers several benefits:

- Fastest path to hybrid-cloud benefits.
- Offloads IT management of infrastructure. Provides an administration experience that puts IT in control without the management and maintenance challenges.
- Enables you to rapidly scale work solutions.
- Provides a separate Azure subscription that is managed and maintained by Citrix. This Isolates activity from your other Azure subscriptions.
- You retain the flexibility to create and manage workloads using your own Azure subscriptions. Your deployment can include workloads that use the Citrix Managed Azure subscription, and workloads that use your own (customer-managed) Azure subscriptions.
- Uses a true consumption-based Infrastructure as a Service (IaaS) model.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Several technologies are available to create connections to your own on-premises networks (such as Azure VNet peering and Azure VPN gateway). This allows your users to access your network's resources, such as file servers.

Deploying and managing Citrix Managed Azure from this service uses the Quick Deploymanagement interface.

For more information, contact your Citrix representative.

Delivering applications and desktops to users

Citrix® StoreFront and Citrix® StoreFront Cloud

StoreFront and Citrix® StoreFront Cloud are the access tiers, providing a user interface for end users to view and launch apps and desktops. Within StoreFront and Citrix® StoreFront Cloud you can define one or more stores, each with a URL. End users can access these stores using Citrix Workspace app or a web browser.

- Citrix® StoreFront Cloud is the Citrix managed access tier. Once you have provisioned DaaS, **Citrix® StoreFront Cloud** is available on the main menu. You must configure the URL, authentication and other configuration. For more information, see Get started with Citrix® StoreFront Cloud.
- StoreFront is the customer managed access tier. You can install StoreFront on servers on your corporate network. End users can connect directly to stores hosted by StoreFront over the network. You can provide remote access using a Citrix Gateway. StoreFront can use Local Host Cache to provide access to resources when DaaS is not reachable. For more information, see Get started. See User access for considerations for using StoreFront in a service environment.

You can use both access tiers. For example you could use Citrix® StoreFront Cloud for remote access, while deploying on-premises StoreFront for areas of your corporate network that need increased resiliency against network outages.

Citrix Workspace app

From the user side, Citrix Workspace app is installed on user devices and other endpoints, such as virtual desktops. Citrix Workspace app provides users with secure, self-service access to documents, applications, and desktops from any device, including smartphones, tablets, and PCs. Citrix Workspace app provides on-demand access to Windows, web, and Software as a Service (SaaS) applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For devices that cannot install Citrix Workspace app software, Citrix Workspace app for HTML5 provides a connection through a HTML5-compatible web browser.

Citrix Workspace app is available for various operating systems. For details, see Citrix Workspace app.

Service Level Agreement

Citrix DaaS is designed using industry best practices to achieve cloud scale and a high degree of service availability.

For complete details about Citrix's commitment for availability of Citrix Cloud services, see the Service Level Agreement.

Performance against this goal can be monitored on an ongoing basis at `<https://status.cloud.com>`.

Limitations

The calculation of this Service Level Goal will not include loss of availability from the following causes:

- Customer failure to follow configuration requirements for Citrix DaaS documented in the product documentation on `<https://docs.citrix.com>`.
- Caused by any component not managed by Citrix including, but not limited to, customer controlled physical and virtual machines, customer installed and maintained operating systems, customer installed and controlled networking equipment or other hardware; customer defined and controlled security settings, group policies and other configuration policies; public cloud provider failures, Internet Service Provider failures or other external to Citrix control.
- Service disruption due to reasons beyond Citrix control, including natural disaster, war or acts of terrorism, government action.

More information

- Citrix DaaS diagrams
- Citrix DaaS Reference Architecture and Deployment Methods
- Technical security overview
- Network ports
- Third-party notices

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- System requirements
- Features
  - An introduction to HDX technologies, plus details about Devices, Graphics, and Multimedia.
  - Remote PC Access: Allow users to log on remotely from anywhere to a physical PC in the office. You can configure Remote PC Access using Studio.
  - Publish content: Publish an application that is simply a URL or UNC path to a resource.
  - Server VDI: Deliver a desktop from a server operating system for a single user.
- For Citrix DaaS Standard for Azure, see its dedicated product documentation.
- To learn about feature availability in the Citrix DaaS products and editions, see the Citrix DaaS feature matrix.
- The Citrix Cloud Learning Series offers education course to get you up and running with Citrix Cloud and its services. You can sequentially view all of the modules, from introductions through planning and building services. You can also choose individual modules or task-specific segments within a module. See Cloud Learning Series.

Get started

To learn how to set up your deployment, start with Plan and build a deployment. That summary guides you through the major steps in the process, and provides links to more information and detailed procedures.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

A goal of Citrix® is to deliver new features and product updates to Citrix DaaS™ customers when they are available. New releases provide more value, so there's no reason to delay updates. Rolling updates to Citrix DaaS are released approximately every three weeks.

This process is transparent to you. Initial updates are applied to Citrix internal sites only and are then applied to customer environments gradually. Delivering updates incrementally in waves helps ensure product quality and maximize availability.

It is possible that the updates mentioned in this documentation are being rolled out and are not accessible to all customers at the same time.

For details about the Service Level Agreement for cloud scale and service availability, see Service Level Agreement. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

Use these articles to learn about release updates, known issues, deprecations and removals, and features in preview:

- What's new lists new and enhanced features in recent releases.
- Known issues lists issues that might affect deployments.
- Deprecations and removals gives advance notice about features that are deprecated, removed, or planned for removal.
- Features in preview lists preview features available for non-production or limited production environments and provides a way to submit feedback.

What's new

This article lists new and enhanced features for Citrix DaaS™. Updates are organized by release month.

Virtual Delivery Agents (VDAs)

VDAs for Windows machines generally are released at the same time as the Citrix Virtual Apps and Desktops™ product.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For information about new VDA and HDX features, see the What's new and Known issues articles for the current Citrix Virtual Apps and Desktops release.
- For information about VDA platforms and features that are no longer supported, see Deprecation. That article also includes platforms and features that will not be supported in a future release (such as which operating systems support VDA installation).

IMPORTANT:

If the Personal vDisk (PvD) component was ever installed on a VDA, that VDA cannot be upgraded to version 1912 LTSR or later. To use the new VDA, you must uninstall the current VDA and then install the new VDA. (This instruction applies even if you installed PvD but never used it.) For details, see If the VDA has Personal vDisk installed.

August 2026

New and enhanced features

Thresholds. Monitor now supports configurable thresholds for system metrics. Define Critical, Warning, and Healthy states for metrics such as CPU usage, memory usage, ICA RTT, network latency, and logon duration across data sources including Machines, Sessions, Cloud Connectors, Provisioning Services, and StoreFront. Color-coded indicators appear on the Dashboard, Infrastructure, Filters, and User/Machine Details pages. Create custom thresholds for specific workloads, or use predefined thresholds with dynamic defaults that automatically adapt to your environment.

For more information, see Thresholds

Citrix Advisor: Scheduled runs and Home page widget. Advisor now runs site checks automatically on a recurring weekly schedule. Each run generates a report retained for up to 90 days.

Also, a new **Advisor** widget on the **Home** page displays a summary of recommendations grouped by impact level and filterable by category, so you can quickly identify and act on critical items.

For more information, see Check for recommendations and Advisor widget.

Microsoft Entra single sign-on. Starting with VDA version 2607, you can use the Microsoft Entra single sign-on machine policy setting to enable or disable this capability on your session hosts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web sign-in (Preview). You can enable web-based sign-in to log in or unlock your Entra joined or Entra hybrid joined virtual desktop. See Web sign-in for details.

Connector Appliance to backend application latency in the Application Topology. The Secure Private Access Application Topology now shows a **Connection Latency** value on the link between the Connector Appliance and the backend application, completing the hop-by-hop latency view. The value is a synthetic P90 round-trip time that the Connector Appliance measures over the past hour. Currently, this covers cloud deployments.

For more information, see Connector Appliance to backend application latency.

July 2026

New and enhanced features

Machine catalog experience enhancements in Studio. We enhanced the machine catalog experience in Studio by displaying the configured naming scheme in the machine catalog details and optimizing the action bar based on usage frequency. **View Machines** is now a top-level action while **Delete Machine Catalog** has been moved to the **More** menu due to its infrequent use.

For more information, see Manage machine catalogs.

Citrix Advisor: New checks for reliability, performance, and operational excellence. Citrix Advisor now includes the following new environment checks that provide actionable recommendations to help improve reliability, performance, and operational excellence:

- Reliability
  - Check Cloud Connector communication with StoreFront
- Performance
  - Place StoreFront servers in a low-latency network
- Operational excellence
  - Review machines in maintenance mode for extended periods
  - Reduce troubleshooting time with Always On Tracing

These enhancements help you proactively identify issues and take corrective actions. For more information, see Citrix Advisor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Extend configuration log search to include low-level operation details. You can now extend the search scope in the **Logging** section of **Web Studio** to include low-level operation details. By selecting **Extend search scope to include details**, you can search low-level details, such as machine name, VDI name, and so on.

For more information, see View configuration log content.

Exclude draining machines from Autoscale capacity buffer. You can now exclude machines that are draining due to scheduled restarts from the Autoscale capacity buffer calculation for multi-session OS delivery groups. When this option is enabled, only machines that are fully available to accept new sessions are counted when determining required capacity. This helps prevent over-provisioning that can occur when draining machines are included in the buffer.

For more information about configuring the option using Web Studio, see Schedule-based and load-based settings.

Alternatively, for configuring using PowerShell, see Exclude draining machines from autoscale calculations.

Deep links from Citrix Aidrien to DaaS. When you ask Citrix Aidrien about machines or sessions, responses now include deep links to the corresponding DaaS console view with search filters applied automatically. This lets you jump directly from a chat response to the relevant interface without manually navigating or rebuilding filters.

Scope support for zones. You can now apply scope control to zones (known as resource locations in Citrix Cloud). This enhancement extends existing scope control capabilities in Citrix DaaS to the zone objects, allowing you to grant custom administrators scoped access to specific zones. With this support, you can align administrative access more closely with your organization's operational and security requirements. For more information, see Assign scopes to a zone.

Set up BYOL separately after connecting your AWS account. You can now connect an Amazon Web Services (AWS) account to Web Studio without configuring Bring Your Own License (BYOL) support during the account connection process. Previously, BYOL setup was a required step in the **Connect AWS account** wizard when connecting to a BYOL-enabled region. Now you can connect your account first, then configure BYOL support at any time by selecting **Set up BYOL** from the **Accounts** list or from the account detail panel. The **Set up BYOL** wizard guides you through enabling BYOL in the AWS WorkSpaces Console and importing a Windows 10 or 11 desktop image for your Citrix on Amazon WorkSpaces Core deployment.

For more information, see Set up BYOL for your account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Faster domain selection with search. Finding Active Directory domains and organizational units (OUs) is now faster in Web Studio. During machine catalog creation, when you select **Create new Active Directory accounts**, you can search for a specific domain directly from the **Location (domain)** drop-down list instead of browsing the full list of trusted domains.

For more information, see Identity pool of on-premises Active Directory joined machine identity.

Task Center: Recurring tab and enhanced task management. Task Center now includes a **Recurring** tab that shows tasks scheduled to run periodically or in the future. In addition to the existing **Recent tasks** tab, which shows individual task runs from the past 90 days, you can now:

- Search and filter both recent and recurring tasks.
- Track real-time task status and recurring schedule state.
- Perform actions on recent tasks, such as cancel or rerun.
- Perform actions on recurring schedules, such as edit or delete.

For more information, see Monitor and manage tasks in Task Center.

Restrict VDA upgrades to tagged machines. You can now limit catalog-level VDA upgrades to a specific subset of machines by using machine tags in Web Studio. When scheduling an upgrade, select **Upgrade machines that match the tag**, choose a tag, and only machines with that tag are included.

This helps support ring-based upgrade strategies where administrators validate a new VDA version with a pilot group before rolling it out to the full catalog.

For more information, see Upgrade VDAs using VUS.

Select Azure replication regions when creating an image version. Studio now includes an **Image Share** page during image version creation, where you can select one or more Azure regions to automatically replicate the prepared image to. You can select resources from different hosting connections and optionally assign a regional disk encryption key. This page appears only when **Store image versions in Azure Compute Gallery** is enabled on the image definition. For more information, see Create image versions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 2026

New and enhanced features

Access Citrix DaaS data in Aidrien. Aidrien can retrieve and display Citrix DaaS environment data directly within the chat, allowing you to investigate issues and manage resources without leaving the conversation. Using natural language, you can search for and view information about:

- Machines and sessions
- Machine catalogs
- Delivery groups

Aidrien presents the retrieved data directly in the chat UI, making it easier to explore your environment, identify issues, and gather information during troubleshooting workflows.

For more information, see Access Citrix DaaS data in Aidrien.

App protection reporting in Citrix Monitor. Real-time reporting of protection policy activations and security risk detections is available in Citrix Director and Monitor. The reporting enables you to quickly assess the risk and configure your protection policies to ensure a safer environment. By proactive risk management and policy reconfiguration, you can strengthen endpoint security in your environment and reduce exposure to emerging threats. For more information, see Endpoint Security policy activation & threat detection reporting

Azure SSD Storage Types for Ephemeral OS Disks. Studio now allows Azure Machine Catalogs that use Azure Ephemeral OS Disks to select the base OS managed disk storage type (Premium SSD, Standard SSD, or Standard HDD) during catalog creation and subsequent catalog/scheme updates, with UI validation and preflight checks to prevent unsupported configurations. For more information, see Use Azure ephemeral OS disk.

Endpoint OS Version Visibility. You can now more effectively manage and track user sessions and connections through enhancements to the Session and Connection pages. These pages now include an Endpoint OS Version column and a corresponding filter for Windows and Linux devices.

This helps you to:

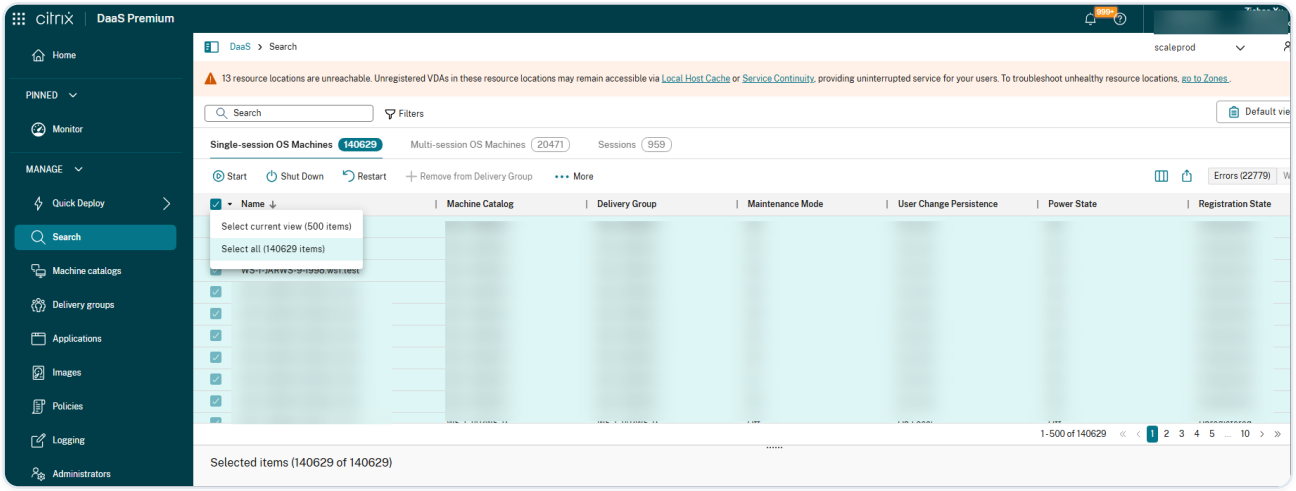
- View the endpoint operating system version directly on the Session and Connection pages.
- Filter sessions or connections based on specific Windows or Linux operating system versions.

For more information, see Endpoint OS Version Visibility

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved bulk actions in Web Studio. You can now select all items across all pages or only within the current page. This enhancement removes the previous 500-item limit for bulk operations on matched search results, improving administrative efficiency in large environments with thousands of VDAs or sessions.

Performance optimizations have also been implemented to ensure bulk actions remain smooth and responsive at scale.



Topology view expanded for Chrome Enterprise Premium and improved policy-evaluation data quality. Citrix Monitor now shows six Chrome Enterprise Premium topology variants spanning cloud and hybrid deployments across internal, external, and external fixed-IP application routes. The **Policy Evaluation** pane can also carry **Application Name**, **Application Type**, **Policies**, and **Security Controls** values over from enumeration events when an app launch event omits them; the **Data path** field can render empty when the source event does not specify it.

For more information, see Chrome Enterprise Premium topology variants.

Image management support prepared image searching

You can now use a search bar in the **Images** node to filter and find image versions by criteria including image definition name, image version number, image version description, OS type, hypervisor type, host connection name, host unit name, host connection type, master image name, provisioning scheme count, and version creation time. This enhancement helps administrators efficiently manage images across large deployments.

For more information, see Image management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for creating Citrix Provisioning catalogs in OpenShift virtualization environments using Studio

With Studio, you can now create Citrix Provisioning catalogs in OpenShift virtualization environments. Previously, you had to switch between different consoles to provision and manage those catalogs. This feature simplifies the process, letting you perform provisioning and power management tasks entirely within Studio.

For more information see, Create Citrix Provisioning™ catalogs in Citrix Studio.

Support for creating Citrix Provisioning catalogs in Citrix Web Studio for Nutanix AHV Prism Central

You can now create a Citrix Provisioning catalog using Web Studio with the Nutanix AHV Prism Central host connection type.

This implementation offers the following advantages:

- A single console to manage both MCS and Citrix Provisioning catalogs.
- New features for Citrix Provisioning catalogs, such as identity management.

For more information see, Create Citrix Provisioning™ catalogs in Citrix Studio.

May 2026

New and enhanced features

Studio support for controlling the visibility of packaged applications. With Studio, you can now control the visibility of a packaged application—on a desktop, on **Citrix Workspace > Apps**, or both. To change visibility for a specific packaged app, go to the **Applications** node, select the application, and choose **Properties > Delivery**.

By default, packaged applications are delivered only on **Citrix Workspace > Apps**. For more information, see Change application properties.

Ability to see sessions and component score and correlate with session performance. Session experience overview is now available on Monitor dashboard. The experience summary provides insights into the number of sessions analysed over a given time-period and the categorisation of the analysed sessions into Good, Medium, and Bad. Session categorisation is done based on the session scores. For the quick snapshot of the overall environment health, the summary also includes the average session score and average component score of the analysed

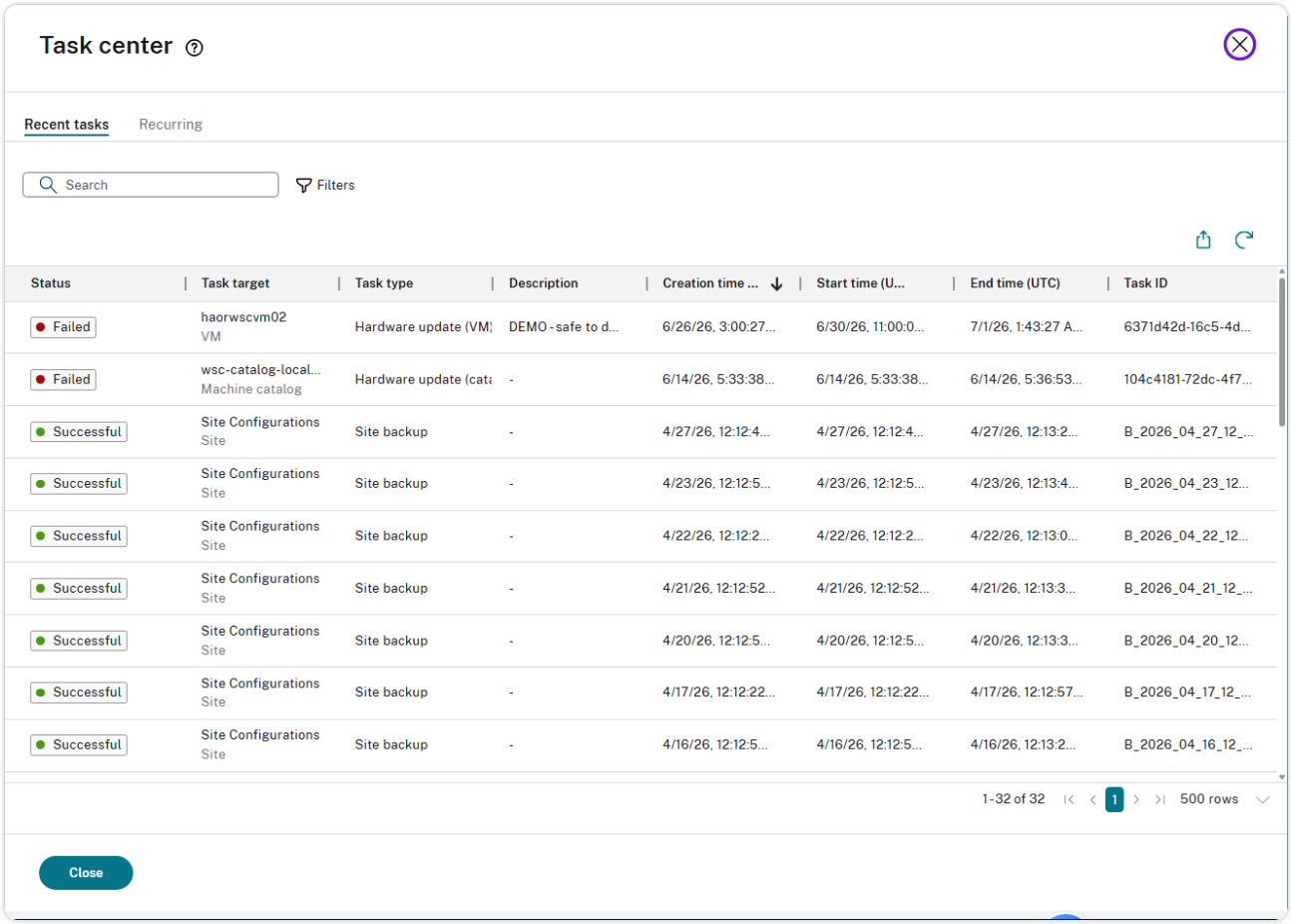
© 1997–2026 Citrix Systems, Inc. All rights reserved.

sessions. Component score can be utilised for troubleshooting session performance, as it provides an additional layer of details for the analysis. For more information, see Session Score

Support for Numecent Cloudpaging applications. You can now discover and publish Numecent Cloudpaging apps using the **App packages** node in Web Studio. You can also store Numecent Cloudpaging application containers on a network file share of your choice and discover and deliver them to end users in Studio by specifying the file share path. This capability simplifies application discovery and expands your options for moving away from App-V infrastructure. For more information, see Cloudpaging applications.

Task Center now available. Task Center provides a centralized view of scheduled and recurring tasks in Studio, helping you track these task statuses: Scheduled, Completed, Failed, or About to run. You can access Task Center by selecting the calendar icon in the upper-right corner of the Studio console.

For more information, see Monitor and manage tasks in Task Center.



Resource filtering. The resource filtering feature lets you configure rules to control user access to resources across delivery groups. You can define the resource type (application, desktop, or both), apply tag restrictions, and set conditions for rule enforcement based on factors like network location and store connection context. To access the feature, go to **Delivery groups > Settings >**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Resource filter. For more information, see Restrict user access to resources across all delivery groups.

Amazon WorkSpaces Core Managed Instances: Studio support for MCS I/O (MCSIO) write-back cache. You can now configure MCS Storage Optimization (MCSIO) write-back cache (WBC) settings directly in Citrix Studio when creating or editing machine catalogs for Amazon WorkSpaces Core Managed Instances. Previously, configuring write-back cache was only avialable through PowerShell commands. Studio now exposes write-back cache options on the Disk Settings page of the Machine Catalog Setup wizard, including cache disk size, memory allocation, EBS storage type (e.g., gp2, gp3, io1, io2), disk persistence across power cycles, and OS disk retention for faster boot times. For more information, see MCSIO enabled catalog.

April 2026

New and enhanced features

Microsoft Entra single sign-on. The **Disconnect remote session on lock for Microsoft identity platform authentication** is now supported on the single-session VDA. See session lock behavior for details.

Update BDM disks for Citrix Provisioning catalogs. You can now update Boot Device Management (BDM) disks for your Machine Creation Services (MCS)-provisioned Citrix Provisioning catalogs. The BDM disk update helps update the Citrix Provisioning server addresses, and UEFI firmware using Studio or PowerShell. This feature saves administrative effort and keeps your environment current. It simplifies catalog management without recreating virtual machines. It supports Azure, Nutanix AHV Prism Central, VMware, and XenServer environments. For more information, see Update BDM disks.

Update vDisk assignments for MCS-provisioned Citrix Provisioning catalogs. You can now update vDisk assignments for existing MCS-provisioned Citrix Provisioning catalogs using Studio or PowerShell. Previously, you had to recreate catalogs to change vDisks. This enhancement saves you time and effort by letting you manage assignments. You can list available vDisks and assign existing vDisks at the catalog level. This feature applies to Azure, Nutanix AHV Prism Central, VMware, and XenServer environments. Note that the vDisk lifecycle management remains within the Citrix Provisioning console. For more information, see Update vDisk assignment.

Reset OS disk for persistent VMs in Nutanix AHV Prism Central. With this feature, you can now reset OS disk for persistent VMs using the `Reset-ProvVMDisk` PowerShell command in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nutanix AHV Prism Central environments. For more information, see Reset OS Disk for Persistent VMs.

Citrix Advisor: New checks for security, reliability, performance, and operational excellence. Citrix Advisor now includes the following new environment checks that provide actionable recommendations to help improve security, reliability, performance, and operational excellence for StoreFront, VDAs, and Active Directory:

- Security
  - Address VDA security vulnerabilities
  - Address Citrix Workspace app security vulnerabilities
  - Upgrade StoreFront server versions that reached End of Life
  - Use HTTPS for StoreFront base URL
  - Use HTTPS for communication between StoreFront and Cloud Connectors
  - Review StoreFront stores with anonymous access enabled
- Reliability
  - Ensure StoreFront server redundancy
- Performance
  - Enable socket pooling for StoreFront stores
- Operational excellence
  - Reset tainted Active Directory accounts
  - Replace deprecated beacon point for StoreFront
  - Disable XenApp Services URL for StoreFront stores
  - Deprecate unsupported StoreFront sites
  - Disable Kerberos delegation for StoreFront stores

These enhancements help you proactively identify issues and take corrective actions. For more information, see Citrix Advisor.

Granular dismissal for Citrix Advisor recommendations. Citrix Advisor now supports granular dismissal, allowing you to dismiss specific affected items within a recommendation rather than having to dismiss the entire recommendation. This enhancement is useful for environments where

© 1997–2026 Citrix Systems, Inc. All rights reserved.

some resources, such as test, validation, or temporary resources, are expected to deviate from best practices.

By dismissing only intentionally non-compliant items, you can reduce noise while maintaining visibility into genuine issues and continuing to receive best-practice guidance for your production resources.

This feature is available for the following resource types:

- Machine catalogs
- Delivery groups
- Application groups
- Zones

For more information, see Dismiss specific affected items in a recommendation.

Customize Advisor check rules. You can now customize Advisor check rules for three key recommendations:

- **Enhance Cloud Connector hardware:** Adjust thresholds for CPU, memory, and disk usage, and exclude specific disks.
- **Release unused resources:** Set custom unused time thresholds for machines and applications.
- **Optimize GPO configuration for VDAs:** Modify GPO processing time duration.

Customized recommendations are labeled with **Customized** for easy identification. You can revert to default settings anytime. For more information, see Customize Advisor check rules.

Control application package update behavior with Preferences. You can now control how application packages are updated in the **Studio > Application Packages** workflow by using new **Preferences** settings. These settings let you preserve user favorites during upgrades, prevent unintended downgrades, and automatically remove obsolete packages during update checks. This helps you maintain a clean and consistent application environment with less manual effort.

For more information, see Upload application packages into your environment.

Cloud Connector visibility for VDAs. You can now see which Cloud Connectors your VDAs are proxied through in **Web Studio > Search**. Use the new **Cloud Connector** column and filter to quickly view and filter VDAs by Cloud Connector. To display the **Cloud Connector** column in the main Search view, select **Columns to display** in the top-right corner.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add notes for power actions. You can now add optional notes when you perform power actions on machines and sessions. These notes help you and other administrators understand the reason for the action. They are recorded in logs for auditing purposes. Notes are supported for the following actions:

- **Machine Actions**:
  - Start
  - Shut down
  - Restart
  - Force restart
  - Force shut down
- **Session Actions**:
  - Log off
  - Restart (single-session)
  - Shut down (single-session)

Support for creating Citrix Provisioning catalogs in Red Hat OpenShift and Nutanix AHV Prism Central virtualization environments using Studio. With Studio, you can now create Citrix Provisioning catalogs in Red Hat OpenShift and Nutanix AHV Prism Central virtualization environments. Previously, you had to switch between different consoles to provision and manage those catalogs. This feature simplifies the process, letting you perform provisioning and power management tasks entirely within Studio. For more information see, Create Citrix Provisioning™ catalogs in Citrix Studio.

Azure ZRS disk types for prepared images. MCS in Azure now enables you to select Zone Redundant Storage (`ZRS`) disk types for prepared images with MCS image management. This enhancement provides greater flexibility in disk type selection and improves the resiliency of your MCS machine catalogs in Azure by ensuring higher availability for prepared image disks.

This helps you to:

- Have prepared image disks with higher availability.
- Avoid the risk of losing prepared images due to zone outages.
- Maintain ongoing operations without impact from storage-side disk failures.

For more information, see Create a prepared image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for image management in Nutanix AHV Prism Central environments. Image management functionality is now generally available for OpenShift virtualization environments. This implementation significantly reduces the storage and time costs, and simplifies the VM deployment and image update process. Currently, you can also PowerShell commands to achieve this goal. For information, see Create catalogs using prepared images in Nutanix AHV Prism Central.

Support for Amulet Hotkey CoreStation plug-in (Preview). With this feature, Citrix manages your Amulet Hotkey CoreStation workloads through a Amulet Hotkey CoreStation plugin. With this plug-in, you can create hosting connections to your Amulet Hotkey CoreStation enclosure, create catalogs, and power manage machines in the catalog using PowerShell commands.

For more information, see:

- Amulet Hotkey CoreStation virtualization environments
- Connection to Amulet Hotkey CoreStation
- Create an Amulet Hotkey CoreStation machine catalog
- Power manage Amulet Hotkey CoreStation VMs

Support for creating MCSIO-enabled MCS machine catalogs of Amazon WorkSpaces Core Managed Instances. You can now create MCSIO-enabled MCS catalogs to create MCSIO-enabled MCS machine catalogs of Amazon WorkSpaces Core Managed Instances to improve write IOPS by directing write operations to the write-back cache and to reduce the startup time when the persisting OS disk is enabled. For more information, see MCSIO enabled catalog.

Manage on-premises image replication. This enhancement introduces an explicit image replication workflow for on-premises hypervisors. Previously, you were not able to replicate image version instances to newly added or superseded storage locations, making it difficult to manage image availability across all necessary storage. With this enhancement, you can run PowerShell commands and replicate the image version instance to storage locations. This feature applies to on-premises hypervisors, including VMware, XenServer, and Nutanix AHV Prism Central environments.

For more information, see Image Replication of additional storage for supported on-premises hypervisors.

Azure SSD storage for ephemeral OS disks. This feature enhances ephemeral OS disk performance in Azure by allowing you to select higher-tier SSD storage types. Previously, only `Standard_LRS` was supported. Now, you can use `StandardSSD_LRS` or `Premium_LRS` by setting the `StorageType` custom property when creating an MCS catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This helps you to:

- Achieve a higher SLA with improved reliability.
- Experience significantly higher IOPS compared to `Standard_LRS`.

For more information, see Configure storage type used by ephemeral disks.

Enhance Azure backup SKU mix. This enhancement removes previous limitations in Azure's `BackupVmConfiguration` feature. Previously, you can't mix VM SKUs that support hibernation with those that do not support it within the same backup list. This update allows you to include both hibernate-capable and non-hibernate-capable SKUs in your backup configurations.

This helps you to:

- Use a broader range of VM SKUs in your backup configurations.
- Improve VM provisioning and start success rates on Azure.
- Increase the resilience of your deployments.

For more information, see Configure backup VM sizes.

Ability to bypass Cloud Connectors for Amazon WorkSpaces Core API requests. When using Amazon WorkSpaces Core Managed Instances, you can now configure host connections to bypass Citrix Cloud Connectors for AWS API requests. This allows MCS to communicate directly from the Delivery Controller to AWS services for provisioning and power management operations instead of routing through a proxy.

This enhancement provides greater operational flexibility, reduces the compute load on Cloud Connector VMs, and removes MCS dependency on Cloud Connectors for AWS API requests. For more information, see Bypass Cloud Connectors for AWS API requests.

Change Azure VM availability zones. This enhancement allows you to modify the availability zone property for existing MCS provisioned VMs in Azure. Previously, this required recreation of the VM. This feature provides greater flexibility, especially for persistent virtual machines.

This helps you to:

- Adjust existing Azure VMs to have no availability zone affinity.
- Assign a specific availability zone to Azure VMs that currently lack one.
- Move an existing Azure VM from one availability zone to another.

For more information, see Update provisioned machines to current provisioning scheme state.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GPU Support in OpenShift MCS. OpenShift MCS currently supports GPU configuration through passthrough behavior. The GPU settings defined on the master VM or in the Machine Profile are read and applied to the VMs provisioned through the MCS catalog. Currently, you can't modify GPU parameters during catalog creation. The GPU configuration is inherited directly from the source configuration and applied to the provisioned VMs as configured.

Flexible billing for Amazon WorkSpaces Core Managed Instances. You can now choose between Monthly (flat-rate) and Hourly (pay-as-you-go) billing models when provisioning Amazon WorkSpaces Core Managed instances using Citrix MCS.

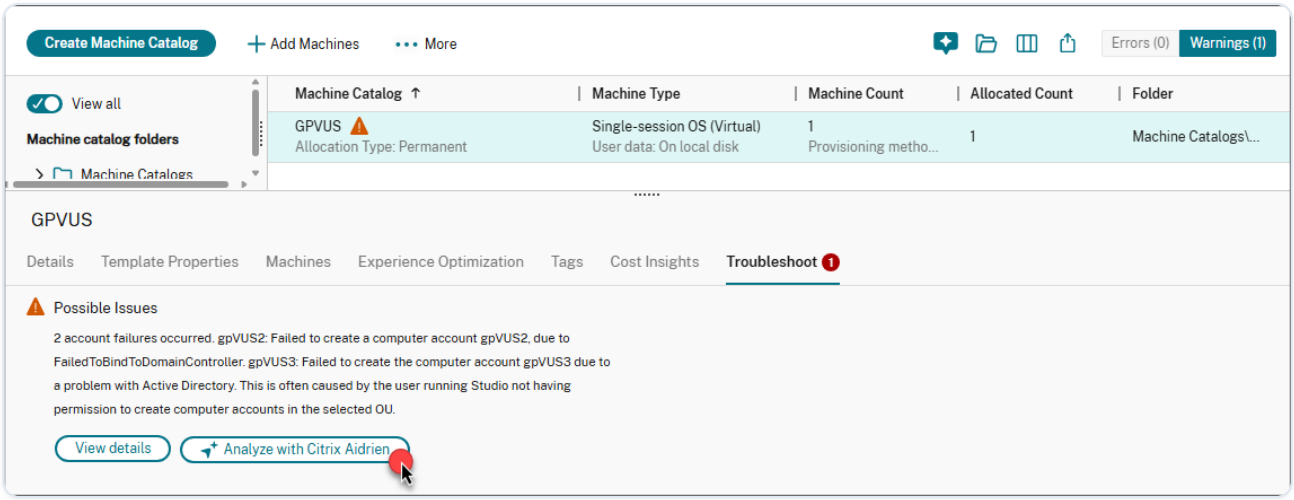
This flexibility allows you to optimize compute costs based on your specific workload requirements and usage patterns.

Use the Monthly billing mode for persistent desktops to benefit from predictable, flat-rate pricing, or use Hourly billing for on-demand or intermittent workloads.

This feature requires your AWS account to be configured for the Amazon WorkSpaces billing service.

For more information, see Flexible billing.

Troubleshoot with Citrix Aidrien. You can now troubleshoot warnings and errors in Citrix DaaS using Citrix Aidrien. When warnings or errors occur, Aidrien is available directly from the **Troubleshoot** tab, warning and error popups, and the Notifications center. Aidrien analyzes issues in context and provides guided insights to help you diagnose and resolve problems faster. For more information, see Citrix DaaS use cases.



AWS EC2: Share AWS prepared images across regions. You can now share a prepared image from one region to one or more different regions within the same AWS account. This feature is available for AWS EC2 environments. When you share an image, the underlying AMI is copied

© 1997–2026 Citrix Systems, Inc. All rights reserved.

along with its properties, such as encryption, hibernation, tags, and trusted launch. This helps you to:

- Deploy and manage prepared images across different regions efficiently.
- Create or update machine catalogs in multiple regions using the shared prepared images.
- Maintain consistent image configurations across your AWS deployment.

For more information, see Share prepared images across availability zones and regions.

AWS EC2: Provision workloads in AWS local zones. You can now provision AWS EC2 workloads directly in AWS local zones. This new feature helps you to:

- Provide low-latency access for end-users by deploying Citrix workloads closer to them.
- Improve regional coverage for your Citrix infrastructure in areas not served by full AWS Regions.

You can create a host connection with a hosting unit in a desired local zone and then provision VMs in that local zone.

For more information, see:

- Create a connection using Studio
- Create a machine catalog from the Machine Catalogs node

Support for creating Citrix Provisioning (PVS) catalogs using MCS PowerShell commands with Nutanix AHV Prism Central connection. You can now create Citrix Provisioning catalogs using MCS PowerShell commands in Nutanix AHV Prism Central host connection. This implementation provides you the following advantages:

- A single unified API to manage both MCS and Citrix Provisioning catalogs.
- Have new features for Citrix Provisioning catalogs, such as, identity management solution, on-demand provisioning, and others.

For more information, see PVS documentation.

March 2026

New and enhanced features

Microsoft Entra single sign-on for DaaS. The following enhancements are available:

- Support for hybrid access on Linux is now available with Citrix Workspace app for Linux 2601.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can now register the Citrix Resource and Client applications through the Citrix Cloud portal.
- You can now perform the Azure configuration through Azure portal.

For more information, see Microsoft Entra single sign-on.

Support for Entra ID extension attributes in MCS. You can now integrate Entra ID extension attributes into your MCS environment. These attributes allow you to store unique, custom data directly on your Entra ID device objects. You can thus apply precise conditional access policies by filtering devices with extension attributes. See Supported operators and device properties for filters for creating more filters based on device attributes. The feature is supported for both Microsoft Entra joined and Microsoft Entra hybrid joined identity types.

You can manage your MCS machine catalogs using Entra ID extension attributes (ExtensionAttribute1-15). For this, prepare a Service Principal with `Device.ReadWrite.All` permission. You can create and update an MCS machine catalog with Entra ID extension attributes using both Studio and PowerShell commands.

Extension attributes are assigned to devices (both persistent and non-persistent VMs) when they are registered.

For more information, see:

- Identity pool of Microsoft Entra joined machine identity
- Identity pool of Microsoft Entra hybrid joined machine identity
- Create Microsoft Entra catalogs enrolled in Microsoft Intune
- Create Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune

Nutanix AHV Prism Central: Improve network configuration. This enhancement improves network configuration for MCS catalogs on Nutanix AHV Prism Central host connections. You can now configure network settings by clearly distinguishing between Basic VLANs, Advanced VLANs, and Overlay networks, preventing errors that occurred when mixed types were previously listed together.

This helps you to:

- Reduce errors during machine catalog creation and editing processes.
- Ensure consistent and valid network configurations through new preflight checks.

For more information, see Create a machine catalog using Studio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Share prepared image versions across hosts in the same resource pool in XenServer. You can now use the **Images** node to share image versions across hosts in the same resource pool in XenServer. This implementation ensures consistency and uniformity of images across different hosts, enhancing deployment flexibility and operational efficiency. You can also use PowerShell commands to achieve this goal. For more information, see Create a prepared image machine catalog in XenServer.

Citrix Advisor: New reliability check. Citrix Advisor now includes a new environment check with the recommendation **Enable service continuity for Citrix Workspace**. This check identifies when service continuity isn't enabled and provides guidance to help you enable it. For more information, see Reliability recommendations.

Customize column layout in Search main views. You can now reorder columns in Web Studio to better organize and group related information. Web Studio retains your column order and width preferences, so your customized layout persists across sessions. Currently, this capability is supported in the main views in **Search**.

Service Window. The Service Window feature provides a capability to schedule and automate operations on MCS-provisioned VMs. This feature currently supports various operations such as Reset OS disk and hardware configuration changes using PowerShell. For information, see Service Window.

February 2026

New and enhanced features

Monitor now supports running Scripted Tasks. This includes the ability to execute Citrix built-in scripts and custom scripts, as well as upload custom scripts for execution. This enhancement enables administrators to perform troubleshooting and automate operational tasks directly from Monitor.

Citrix Always on Tracing. Citrix Cloud expands Always On Tracing (AOT) to simplify centralized log collection for Citrix Virtual Apps and Desktops. Configuration is managed through DaaS Settings, where administrators define Log Server details, logging scope, and access controls, with settings applied across the environment.

Citrix Monitor adds a dedicated AOT Logs view with near real-time visibility, search, and filtering by time range, log type, and machine to speed up troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AOT logs are sent to the AOT Log Server from supported components deployed in customer resource locations, including Windows, Linux, and Mac VDAs, StoreFront, Federated Authentication Service (FAS), and Session Recording Server.

For more information, see Always On Tracing.

NOTE:

AOT logs from Citrix Cloud control plane components continue to be sent to Citrix-managed monitoring systems, such as Splunk. Only components deployed in customer resource locations send logs to the AOT Log Server.

Microsoft Entra single sign-on for DaaS. Support for hybrid access on Windows and Mac is now available. See Microsoft Entra single sign-on for details.

Backup VM configuration in AWS EC2. Studio now enables you to define a list of backup EC2 instance types ("Backup SKUs" that can be On-demand or Spot instances) in AWS environments that Machine Creation Services (MCS) can fall back to in case of capacity-related issues. MCS tries to fall back on the backup EC2 instance types in the order that is provided by you in the list. For more information, see Create a catalog using Studio.

Support for Azure Extended Zones. You can now provision workloads in Azure Extended Zones using MCS provisioning. Azure Extended Zones are small footprint extensions of major Azure regions. They provide lower latency and data residency for customers that are further from the main region location. For more information, see Azure Extended Zones.

Red Hat OpenShift: Citrix Provisioning catalog using MCS. This enhancement adds support to the OpenShift Plug-in to provision Citrix Provisioning (PVS) catalogs using MCS.

With this capability:

- The OpenShift Plug-in can be used as a hosting connection for Citrix Provisioning machine catalogs provisioned by MCS.
- Citrix Provisioning target devices can boot using Citrix Provisioning BDM boot, with the BDM disk stored in OpenShift.

For more information, see the Citrix Provisioning document Create Citrix Provisioning™ catalogs in Citrix Studio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enroll HPE Moonshot machines to machine catalogs using WebSocket. You can now register your non-domain joined or Microsoft Entra joined VDAs on HPE Moonshot to machine catalogs using WebSocket. For more information, see Enroll machines to catalogs using the WebSocket VDA enrollment tool.

Support for VMware vVols in MCS. You can now use VMware vVols with MCS on vSphere environments. Previously, creating MCS catalogs on vVols resulted in PBM errors. This update resolves that issue. This integration provides granular control over your MCS virtual machine storage. For information, see Storage Profile.

Use WinHttp (netsh) proxy server settings for hosting connection. This feature allows hosting connections to use the WinHttp (netsh) proxy server settings configured on the Citrix Cloud Connectors to be used with the hosting connection. For more information, see Use WinHttp (netsh) proxy server settings for hosting connection.

Amazon Workspaces Core Managed Instances: Cross-account provisioning using PowerShell. There are use-cases where the Cloud Connectors would like to be placed in a separate AWS account (shared services account or site components account) with IAM roles that have cross-account access (cross-account IAM role) and MCS-provisioned machine catalogs in separate secondary AWS account (workloads accounts), without the need for additional Cloud Connectors in the separate accounts. To support such scenarios, this feature uses VPC peering and cross-account access using IAM roles to make provisioning across different AWS accounts possible for enterprises managing multiple AWS accounts.

With VPC peering, you can have your Cloud Connector, and provisioned VMs in different regions or accounts be able to communicate among each other.

With cross-account access using IAM roles, you allow the primary account (Cloud Connector account) to assume an IAM role to access AWS resources in the secondary account (machine catalog VMs).

For detailed information, see Cross account provisioning.

Amazon Workspaces Core Managed Instances: Provision workloads in AWS local zones. You can now provision Amazon Workspaces Core Managed Instances workloads directly in AWS local zones. This new feature helps you to:

- Provide low-latency access for end-users by deploying Citrix workloads closer to them.
- Improve regional coverage for your Citrix infrastructure in areas not served by full AWS Regions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can create a host connection with a hosting unit in a desired local zone and then provision VMs in that local zone.

For more information, see:

- Create a connection using Studio
- Create a machine catalog from the Machine Catalogs node

Amazon WorkSpaces Core Managed Instances: Share AWS prepared images across regions. You can now share a prepared image from one region to one or more different regions within the same AWS account. This feature is available for Amazon Workspaces Core Managed Instances environments. When you share an image, the underlying AMI is copied along with its properties, such as encryption, tags, and trusted launch. This helps you to:

- Deploy and manage prepared images across different regions efficiently.
- Create or update machine catalogs in multiple regions using the locally shared prepared images.
- Maintain consistent image configurations across your AWS deployment.

For more information, see Share prepared images across availability zones and regions.

Expanded icon support. When customizing icons for desktops and applications in Studio, you can now extract and use icons from `.exe` files, in addition to the previously supported `.ico` format.

You can browse and select those icons from either your local machine or a VDA machine. The maximum supported icon file size is 500 KB. For more information, see Create delivery groups and Manage delivery groups.

Citrix Advisor: New checks for reliability, performance, security, and cost effiency. Citrix Advisor now includes the following new environment checks that provide actionable recommendations to help improve security, reliability, performance, and operational excellence:

- Security
  - Use HTTPS for host connections
  - Upgrade operating systems that reached End of Life
  - Upgrade hypervisor versions that reached End of Life
- Reliability

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Enable advanced health check for StoreFront stores
    - Add all Cloud Connectors as STA servers on StoreFront and NetScaler Gateway
- Performance
    - Optimize GPO configuration for VDAs
    - Evaluate write cache disk size for PVS target devices
- Operational excellence
    - Simplify catalog configuration with a machine profile

These enhancements enable you to proactively identify issues and take corrective actions to maintain a secure, reliable, high-performance, and operationally efficient deployment. For more information, see Citrix Advisor.

Forward Always-on Tracing (AOT) logs to your log server. In Web Studio, you can now forward Always-on Tracing (AOT) logs from Citrix components to a designated log server. This feature enables centralized troubleshooting and more effective monitoring of your Citrix environment. For more information, see Configure the log server settings.

Migrate machine catalogs to Citrix-managed Nutanix AHV Prism Central host connection. With this feature, you can migrate your Citrix machine catalogs, and their associated VMs from existing Nutanix AHV (for Prism Element) and Nutanix AHV PC (for NC2 on Azure) host connections to the Citrix-managed Nutanix AHV Prism Central host connection. For migration, use PowerShell commands, which also include fast rollback options in case of issues, and commands to clean up source resources post-migration. For information, see Migrate machine catalogs to Citrix-managed Nutanix AHV Prism Central host connection.

Use machine profiles for Nutanix AHV Prism Central host connections. You can now use machine profiles to define hardware configurations for VMs provisioned through your Nutanix AHV Prism Central host connection. This new workflow captures properties like CPU, memory, cores per socket, GPU, and categories from the machine profile. You can overwrite CPU, memory, and core per socket configurations during catalog creation or editing. The master image's template version defaults as the machine profile for new catalogs. You can create a new catalog with a machine profile, update an existing catalog, and convert a non-machine profile based machine catalog to a machine profile based machine catalog using Studio and PowerShell. For more information, see:

- Studio

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Create a machine catalog using Studio
    - Add or change the machine profile.

- Powershell

    - Create a machine catalog using PowerShell commands
    - Add or change machine profile

Single-use pooled desktops during LHC events. Power-managed, single-session, pooled desktops are now available for a single use by default during a Local Host Cache (LHC) event. This change ensures that users can access these machines without the concerns about desktop reuse. The existing functionality to configure these desktops for reuse remains unchanged. For more information, see Enable using Studio.

January 2026

New and enhanced features

Discover and deliver Citrix elastic app layers in Studio. You can now discover and publish elastic app layers using the **App packages** node in Studio, including:

- Discover and enumerate a library of elastic app layers authored using Citrix App Layering.
- Create assignment policies to deliver apps elastically to users on non-persistent machine catalogs.
- Deliver portable elastic app layers to any non-persistent Windows machine, regardless of whether the image was published from an App Layering appliance.

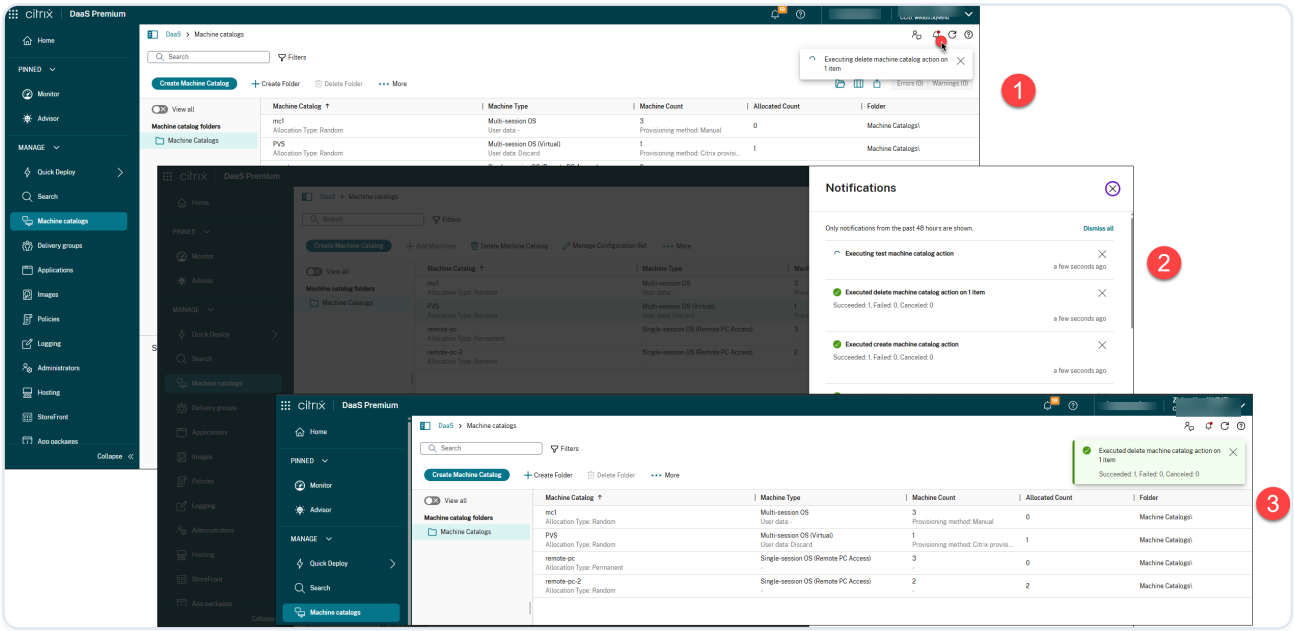
For more information, see Manage app packages.

In-session notifications for background operations. Web Studio now includes a notification center that gives you real-time visibility into background operations and reports on operation results.

When you start a time-consuming operation, a notification appears in the upper-right corner to let you know it's in progress. Operations that previously blocked the UI now run in the background, so you can continue working without interruption. Once the operation completes, a real-time status notification appears, and the result is also saved in the notification center. The notification center maintains a 48-hour history, making it easy to track recent activity.

For more information, see Studio overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft Entra single sign-on for DaaS. Support with new Workspace app platforms and Windows Server 2025 is now available. See Microsoft Entra single sign-on for details.

Follow-me tagging. Follow-me tagging enables tracking of individual end-user VM usage by applying hypervisor-level tags. These tags, labeled with the specific user and/or organization (using `citrix-user-upn` as the key and the User Principal Name (UPN) as the value), are added when a user is assigned to a VM and removed when the user is unassigned.

This feature offers several advantages:

- **IT chargeback**: Facilitates filtering resource usage (Azure: NICs, OS, ID, WBC, Data disks, and VMs) (AWS EC2: EC2 instance, EBS volumes (OS, ID, WBC, and Data disks), Network Interfaces) by tags, allowing for accurate chargeback to individual users or business units.
- **Efficient user management**: Automates the removal of tags from resources when end-users are unassigned due to employment changes like termination or reorganization.
- **Enhanced security monitoring**: Helps identify VMs assigned to specific end-users for targeted security scans.

Currently, follow-me tagging is applicable to:

- AWS EC2 and Azure environments
- Statically assigned machines running single-session OS
- Persistent and non-Persistent catalogs
- All supported machine identity joined catalogs
- Only MCS provisioned VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Managed disks only

For more information, see Follow-Me Tagging.

Support for provisioning data disk in AWS. A data disk allows storage of persistent data like event logs, security traces, and application data.

With this feature, you can now create and assign a persistent data disk to an MCS created persistent or non-persistent VM of an MCS machine catalog in AWS. The source of the data disk must be the master image (AMI's secondary volume). You can provision the data disk using both Studio and PowerShell commands. However, you can provision data disks using Studio UI only when the master image (AMI) has two volumes, OS disk (root volume) and data disk (secondary volume).

For information on creating an MCS machine catalog with a data disk, see Provision a data disk on MCS created VM.

December 2025

New and enhanced features

Azure: Clone MCS catalogs. You can now use the `Copy-ProvScheme` PowerShell command to clone an existing persistent and non-persistent MCS machine catalog in the Azure virtualization environment. This feature creates a new provisioning scheme by copying the details of an existing scheme, including associated configurations, network mappings, and security groups. This helps you to:

- Split an existing single catalog into multiple catalogs to apply different catalog-level policies and configurations.
- Isolate specific virtual machines within a large catalog for quick testing or to treat them separately based on functional roles.

For more information, see Clone an MCS catalog.

Enhanced experience optimization settings for Citrix DaaS. We've enhanced **Experience Optimization** settings to help you easily fine-tune resource allocation and boost performance across machine catalogs. You can now create or select configuration sets for tailored optimization, or quickly apply default settings like automatic CPU spike protection and intelligent CPU optimization.

For more information, see Select a configuration set for experience optimization.

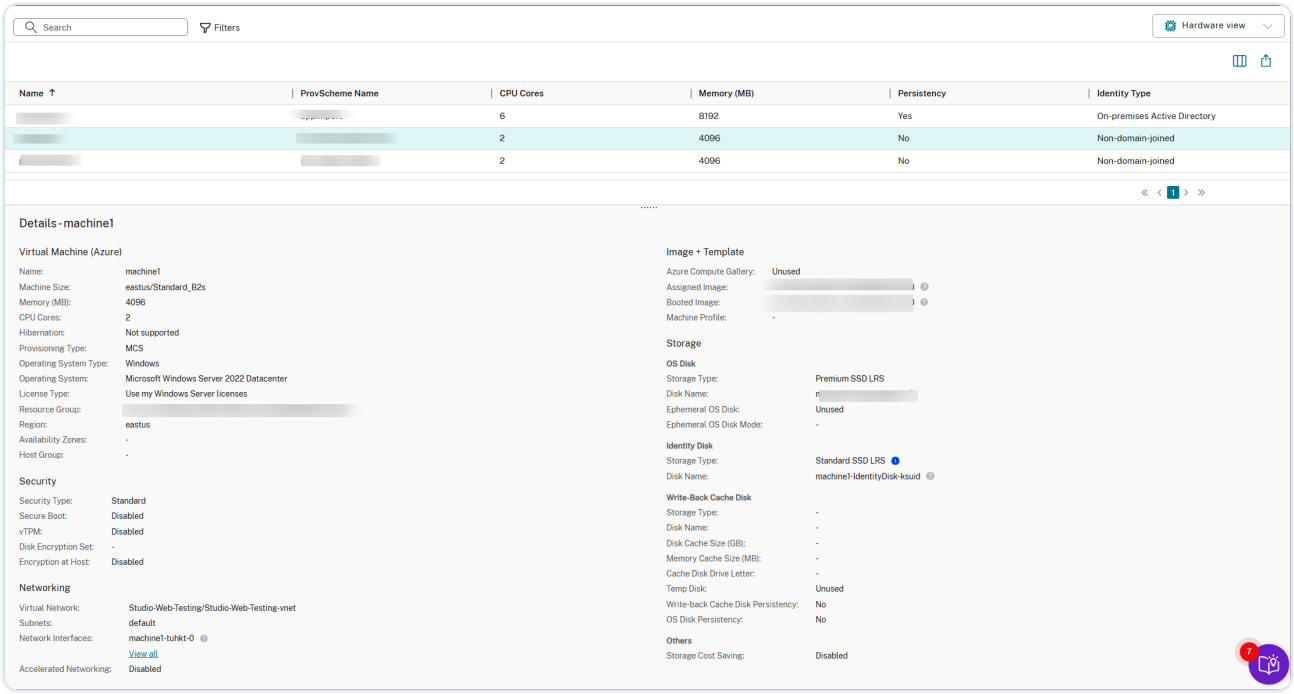
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Machine hardware view in the Search node. You can now access a dedicated hardware view in the Search node for machines provisioned using Machine Creation Services (MCS). This view gives better visibility into machine hardware details and makes managing MCS-provisioned machines easier.

Key benefits include:

- View detailed hardware configurations, including machine size, operation system, license type, security settings, networking, image, template, and disk settings.
- Easily locate machines using hardware filters and search options.

Currently, Hardware view is available for MCS-provisioned machines in VMware, XenServer, SCVMM/Hyper-V, Nutanix PC, Azure, Azure Arc, Azure Local, AWS EC2, and GCP. OpenShift and Amazon WorkSpaces Core currently show basic hardware information as columns only. For more information, see Monitor MCS-provisioned machines in Search > Hardware view.



Improved scope control for Default Policy Set. Scope control has been available for policy sets. To maintain compatibility, **Default Policy Set** is now assigned to *any* scope, with **Bypass scope control** enabled by default. Review your **Default Policy Set** assignments and adjust them if you want to limit access based on scope.

You can update scope assignments in two ways:

- From the policies: Edit the **Default Policy Set** and change its associated scopes.
- From the scope: Go to the scope in **Administrators > Scopes** and assign or remove **Default Policy Set** from it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Create and manage scopes and Create and manage policy sets.

StoreFront node relocation. The **StoreFront** node has been removed from Web Studio. All settings and configuration options previously available in the **StoreFront** node are now available on the **Settings** tab of the **Delivery groups** node. This consolidation simplifies navigation and keeps related configuration options in one place.

AWS EC2: Share prepared images across availability zones. Previously, to create MCS machine catalogs across multiple availability zones, you needed a separate prepared image for each availability zone. This increased your operational complexity to have to manage several prepared images and could lead to potential inconsistencies in image management.

With this feature, you can share a single prepared image across different availability zones within the same AWS region for AWS EC2. This simplifies catalog creation and image updates, reducing management overhead significantly. Currently, use PowerShell commands to manage image sharing. For more information, see Share prepared images across availability zones.

Create MCS provisioned VMs with vTPM enabled in XenServer 8. With this feature in XenServer 8, you can create an MCS machine catalog with vTPM. If machine profile-based configuration is used and vTPM is enabled, then VMs in the catalog inherit the same vTPM content from the VM template. If the machine profile is not used and the master image is vTPM enabled, then VMs in the catalog will inherit the same vTPM content as the master image. For information, see Create a machine profile-based machine catalog using PowerShell.

November 2025

New and enhanced features

Microsoft Entra single sign-on for DaaS. You can now leverage single sign-on (SSO) when using Microsoft Entra ID credentials to access virtual applications and desktops on Microsoft Entra joined or Microsoft Entra hybrid joined session hosts. For more information, see Microsoft Entra single sign-on.

Amazon WorkSpaces Core Managed Instances: Share prepared images across availability zones using Studio UI. With this feature, you can share a single prepared image across different availability zones within the same AWS region for Amazon WorkSpaces Core Managed Instances using Studio UI. Alternatively, you can also use PowerShell commands to manage image sharing. For more information, see Share Prepared Images Across Availability Zones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

One-time use pooled desktops in Local Host Cache. You can now configure one-time use of pooled desktops during Local Host Cache (LHC) outage mode. It leverages a hygiene blob distributed only to VDAs version 2407 and later. Capable machines are automatically scheduled for reboot after a single outage session to guarantee a clean state. This feature improves customer sentiment during outages by making availability more seamless. For more information, see One-time use pooled desktops in Local Host Cache.

Managing prepared image versions in AWS EC2. Image management functionality is now generally available for AWS EC2 virtualization environments. You can use **Images** node to create multiple image versions and apply or update multiple machine catalogs. This implementation significantly reduces the storage and time costs and simplifies the VM deployment and image update process. You can also use PowerShell commands to achieve this goal. For more information, see Create a prepared image machine catalog in AWS EC2.

Amazon WorkSpaces Core Managed Instances non-domain join support in Studio UI. Previously, the Studio UI supported on-premises Active Directory and Microsoft Entra hybrid joined for Amazon WorkSpaces Core Managed Instances, but it did not support provisioning non-domain joined configurations.

With this enhancement, you can provision Amazon WorkSpaces Core Managed Instances that are non-domain joined directly within the Studio UI using MCS. This functionality is supported during both the creation and editing phases of MCS machine catalogs in the Studio UI. For information, see Create a machine catalog from the Machine Catalogs node.

Azure: Support cross-family backup VM sizes for Hibernated VMs. MCS on Azure now supports using cross-family VM sizes for backup configurations in hibernation-enabled machine catalogs, improving resiliency. This feature removes the prior restriction that blocked cross-family fallback to prevent blue screen errors upon resume. When an allocation failure occurs while resuming a hibernated VM, MCS automatically handles the size change, ensuring you still get a working VM. Note that switching the VM size requires clearing the hibernated state, resulting in the loss of the VM's memory state (RAM data). This functionality is available for both persistent and non-persistent MCS catalogs. For more information, see Configure backup VM sizes.

Enhanced workload rightsizing. The enhanced workload rightsizing page helps you analyze the usage and sizing aspects of your delivery groups. Hereby, delivery groups can be analyzed based on machine or user activity.

The machine-based analysis enables you to:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Categorize virtual desktops based on usage to identify machines with no or low activity and reduce spending on unused resources. For more information, see Usage Analysis
- Analyze resource utilization on virtual desktops to identify machines that needs to be right sized to reduce cost or improve user experience.For more information, see Sizing Analysis

The user-based analysis enables you to:

- Categorize the users based on their activity. Consider removing the access entitlement of users with no activity for IT hygiene reasons. Users with low usage could be moved to shared resources for a more efficient use of resources.
- Analyze the resource consumption of users to identify cohorts with higher or lower than average resource consumption, and to distribute users more effectively.

Machine analysis is ideal for scenarios with virtual desktops statically assigned to users, such as Windows 365 Enterprise or Frontline dedicated. User analysis is useful for the analysis of delivery groups with randomly assigned virtual desktops. Both analyses are currently limited to single session machines.

NOTE:

The classic rightsizing analysis, accessible through the “All Workloads” button at the top of the page, will be deprecated in an upcoming release.

View users blocked by session launch failures. Administrators now have **visibility into users blocked by session launch failures**. This new summary is available within the **Filters** under the **Connections** view, enabling improved prioritization and analysis of failures.

Session performance trends are now available with customization. The Session Performance trends in Citrix Director supports historical data. Administrators can now customize the metrics to correlate from an enriched list of performance metrics.

Diagnostic insights on machines and sessions for Proactive monitoring. Citrix Director now features an Insights panel to help administrators proactively identify and resolve session failures and performance issues. This powerful tool provides diagnostic insights, refreshed every 15 minutes, to highlight problematic machines and sessions impacting your site.

Key insights include:

- Black Hole machines: Detects machines that fail to service consecutive session requests

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Zombie sessions: Identifies single-session OS machines with abandoned sessions that block new session launches.
- Overloaded machines: Flags machines with sustained CPU or memory spikes that are degrading user experience.
- Connection failures: Highlights client and server failures, providing details on failure patterns and user impact.

The insights are customizable, with alert policies that can be configured for notification. Insights empower administrators to be proactive, take timely action, and improve session availability and performance across their environment. For more information, see Insights

October 2025

New and enhanced features

Citrix Advisor: New checks for reliability, performance, security, and cost efficiency. Citrix Advisor now includes the following new environment checks that provide actionable recommendations to help improve reliability, performance, security, and cost efficiency:

- **Reliability**
  - Enable communication between Cloud Connectors for reliable LHC performance
  - Place Cloud Connectors in the same domain
  - Check resiliency configurations
- **Performance**
  - Rightsize high resource-consuming machines
  - Reduce the number of host connections in your zones
  - Reduce the number of VDAs in your zones
  - Evaluate resource allocation for PVS servers
  - Increase resource allocation for PVS servers
  - Optimize Cloud Connectors for LHC mode
- **Security**
  - Upgrade Citrix Workspace app versions that reached End of Life
  - Assign resources to security groups

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Cost optimization**
  - Release unused resources

These enhancements help you proactively identify issues and take corrective actions to maintain a reliable, secure, and cost-effective environment. For more information, see Citrix Advisor.

Provision persistent workloads of Amazon WorkSpaces Core Managed Instances. Previously, you could only use MCS to provision non-persistent workloads of Amazon WorkSpaces Core Managed Instances. With this new capability, you can create a persistent catalog of Amazon WorkSpaces Core Managed Instances using MCS. User writes and changes to their desktops are persisted on the OS disk (root volume) between different boots of their persistent WorkSpaces Core Managed Instance provisioned by MCS.

Note that this workflow differs from using Quick Deploy to provision Amazon WorkSpaces Core Bundles.

For more information, see Create a catalog of Amazon WorkSpaces Core Managed Instances.

Amazon WorkSpaces Core Managed Instances: Share prepared images across availability zones. Previously, to create MCS machine catalogs across multiple availability zones, you needed a separate prepared image for each availability zone. This increased your operational complexity to have to manage several prepared images and could lead to potential inconsistencies in image management.

With this feature, you can share a single prepared image across different availability zones within the same AWS region for Amazon WorkSpaces Core Managed Instances. This simplifies catalog creation and image updates, reducing management overhead significantly. Currently, use PowerShell commands to manage image sharing. For more information, see Share Prepared Images Across Availability Zones.

Share prepared image versions across clusters and vCenters. You can now use the **Images** node to share image versions across hosting connections in VMware. This implementation ensures consistency and uniformity of images across different clusters or vCenters, enhancing deployment flexibility and operational efficiency. Alternatively, you can use PowerShell commands to achieve this goal. For more information, see Image Management and Share prepared images.

Create a secure environment for AWS-managed traffic in Amazon WorkSpaces Core environment. If you have a proxy configured on the Cloud Connectors, then you must create the host connection to use the proxy so that API calls made by MCS are properly routed through the proxy. MCS enables network traffic (API calls from Citrix Cloud to AWS hypervisor) to be routed

© 1997–2026 Citrix Systems, Inc. All rights reserved.

through Cloud Connectors in your Amazon WorkSpaces Core environment using Studio. For more information, see Create a connection using Studio.

Exclude maintenance mode VMs from the autoscale pool. Previously, VMs in maintenance mode were included in the autoscale pool depending on the delivery group. For example, single-session delivery groups included VMs in maintenance mode in the autoscale pool, while multi-session delivery groups excluded them.

With the new desktop group property `PoolSizeExcludesMaintenanceMode`, you can now exclude VMs in maintenance mode from the autoscale pool irrespective of the delivery group. If you set the property to `true`, VMs in maintenance mode are excluded from the autoscale pool. Conversely, if set to `false`, they are included. For more information, see Set-BrokerDesktopGroup.

Enhanced user assignment default for improved security. We've updated the default behavior when assigning users within a delivery group. Restricted control is now the default, ensuring better security and more granular access control. The alternative option, **Allow any authenticated users to use resources**, is now clearly marked as **Not recommended**, and should be used only for specific scenarios like shared or pooled desktops for broad access, kiosk environments, or testing purposes. This change helps reduce risk while giving you flexibility when needed.

For more information, see Configure user scope for an access policy.

Two new service health alerts. Two new site-level alerts are available to help you monitor deployment health:

- Resources are located in the initial zone.
- Advanced health check is not enabled on StoreFront.

To view these alerts, click the flag icon in the upper-right corner of the Home page. For more information, see Studio home page.

Improved application package management. In Studio, you can now choose to automatically remove packages that no longer exist in the source (now called *profile*) location when checking for updates. This new **Remove absent packages** option in the **Preferences** field helps you easily clean up the application packages UI by removing outdated entries from the **Packages** tab.

In addition, several tabs and sections in the App packages node have been renamed to better align with the wider suite of package types now supported in Studio:

- **Add Source** is now **Create discovery profile**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Check for package updates** is now **Check for updates**
- **Remove source** is now **Delete profile**

For more information, see Manage app packages.

Cross-account provisioning in AWS EC2 using Studio UI. There are use-cases where the Cloud Connectors would like to be placed in a separate AWS account (shared services account or site components account) with IAM roles that have cross-account access (cross-account IAM role) and MCS-provisioned machine catalogs in separate secondary AWS account (workloads accounts), without the need for additional Cloud Connectors in the separate accounts. Such a deployment model is already supported using Powershell SDK, and is now also supported using the Studio UI.

Enhanced proxy configuration for AWS EC2 host connections. Previously, MCS was unable to read the system proxy value configured by you on the Cloud Connector to configure a system proxy for an AWS host connection. With this enhancement, AWS host connection can now read the WinHTTP system proxy value that is configured during Cloud Connector installation if you set the custom property `UseSystemProxyForHypervisorTrafficOnConnectors` to `true` when creating or updating a host connection using PowerShell. This enhancement therefore:

- Allows AWS client to read proxy values, enabling proper API calls through the proxy, which is essential for internet communication.
- Reduces the need to manually configure proxy server and port values through CLI.

For more information, see Enhanced Proxy Configuration for AWS host connection.

Multi-select support for key entities using “IN” operator. This enhancement introduces the ability to select multiple values for key filter fields such as users, machines, and delivery groups, utilizing an "IN" operator.

September 2025

New and enhanced features

Support for using AWS EC2 Spot instances. With this feature, you can create an MCS machine catalog of Spot instances (persistent request only) in AWS virtualization environment using machine profile workflow.

Compared to On-demand instances, Spot instances offer cost savings of up to 90%. However, Spot instances may be interrupted by Amazon EC2 if capacity becomes unavailable, making them suitable for non-critical applications and desktops only.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Additionally, with this feature, you can use Spot instances as backup SKUs.

For more information, see Create a catalog using AWS Spot instance.

Scoped Studio access for CSP tenant admins (Preview). As a Citrix Service Provider (CSP), you can now grant your tenant admins access to a lightweight version of the DaaS Studio console directly from their Citrix Cloud console.

Instead of being blocked when selecting Manage DaaS, tenant admins are now taken to a scoped Studio view where they can manage their own objects—such as catalogs and delivery groups—based on federated domain and role-based permissions. Unscoped or global objects like Zones and Tags are hidden to maintain tenant isolation and provide a secure, streamlined self-service experience.

For more information, see Tenant service administration.

Citrix Troubleshoot Connection. The Citrix Troubleshoot Connection feature is designed to empower end-users to effectively self-troubleshoot potential desktop or application launch failures. This enhancement aims to provide users with clear diagnostics, potential recommendations, and the ability to run fixes with a simple click. For more information, see Citrix Troubleshoot Connection.

Improved multi-selection in the Search node. We've updated the **Search** node with a more intuitive table layout. This change enables you to:

- Select multiple items using checkboxes in each row, making the experience more intuitive.
- Select all items on the current page using the checkbox in the column header.

While multi-selection and page-level selection aren't new (previously done using keyboard shortcuts), this enhancement greatly improves affordance and usability, and lays the groundwork for future support of multi-selection across pages.

Session auto reconnect details in Filters view and Session Performance tab. You can now view session auto reconnect details in both the **Filters** > **Sessions** tab and the **Session Performance** tab. This enhancement allows you to quickly access and analyze the number of auto reconnects in a session.

Filters view:

To display the new Session Auto Reconnect column, go to **Choose Columns** and then select **Session Auto Reconnect** in the **Filters** > **Sessions** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A drilldown provides additional information such as Session Reliability or Auto Client Reconnect, timestamps, Endpoint IP, and Endpoint Name of the machine where Citrix Workspace app is installed. This information was previously available in the Trends tab. For more information, see the Historical trends page.

Session Performance Tab:

You can now view session auto reconnect details in the **Last 48 hr** tab of the **Session Performance** tab.

The graph displays the number of Total Session Reconnects, Auto Client Reconnects, and Session Reliability Reconnects.

The auto reconnect information helps you to view and troubleshoot network connections with interruptions and analyze networks for a seamless experience.

Enhanced definitions of ICA RTT and Network latency measurements in Monitor. The definitions and measurement methods for ICA Round Trip Time (RTT) and Network Latency in Director are now enhanced. This update changes the underlying counters and the sampling interval for these metrics. These improvements address previous limitations in how the metrics were reported. You now get more accurate and reliable insights for monitoring user experience in Citrix environments.

Support for image management in Red Hat OpenShift environments. Image management functionality is now generally available for OpenShift virtualization environments. You can use **Images** node to create image definitions, versions, and MCS machine catalogs. This implementation significantly reduces the storage and time costs, and simplifies the VM deployment and image update process. You can also use PowerShell commands to achieve this goal. For information, see Create a prepared image machine catalog in Red Hat OpenShift.

Support for creating Red Hat OpenShift catalogs using machine profile. With this feature, using Studio, you can now create a Red Hat OpenShift catalog in MCS using a machine profile. The input of the machine profile is an existing VM. Creating a catalog using a machine profile allows VMs in the catalog to inherit hardware properties such as CPU count and memory size. For information, see Create a Red Hat OpenShift catalog.

Managing prepared image versions in XenServer. Image management functionality is now generally available for XenServer virtualization environments. You can use **Images** node to create multiple image versions, and apply or update to multiple machine catalogs. This implementation significantly reduces the storage and time costs, and simplifies the VM deployment and image

© 1997–2026 Citrix Systems, Inc. All rights reserved.

update process.You can also use PowerShell commands to achieve this goal. For more information, see Create a prepared image machine catalog in XenServer .

Improve upgrade reliability with a pre-upgrade VDA restart. The VDA Upgrade Service now offers the ability to restart VDAs before the upgrade begins. This helps improve upgrade success rates by starting from a stable system state and avoiding issues caused by pending restarts. For more information, see Upgrade VDAs.

Secure Private Access integration in Web Studio The integration of Secure Private Access (SPA) with Web Studio is enhanced. Administrators in your organization can now open the SPA console directly from the left navigation in Web Studio.

August 2025

New and enhanced features

Multi-select support for delivery groups. The **Delivery Group** drop-downs in the **Sessions** and **Logon Performance** pages under the **Trends** tab are enhanced with:

- Search for delivery group names using text input
- Multi-select up to 15 delivery groups for comprehensive analysis

This enhancement improves usability and allows for more efficient monitoring and comparison across multiple delivery groups simultaneously.

Share prepared image versions across subscriptions and tenants in Azure. You can now use the **Images** node to share image versions across hosting connections in Azure. This implementation ensures consistency and uniformity of images across different subscriptions or tenants, enhancing deployment flexibility and operational efficiency. You can also use PowerShell commands to achieve this goal. For more information, see Image Management.

Improved handling of vertical and horizontal load balancing alerts. Previously, when you set `UseVerticalScalingForRdsLaunches` to true and configured the “Maximum number of sessions” policy in Studio, machines moved to the “Maximum capacity” state. Director triggered alerts for “Maximum capacity” whether the limit was reached due to vertical or horizontal load balancing. There was no way to distinguish between vertical and horizontal load balancing when encountering specific errors, such as "Max Load Reached." This caused unnecessary alerts for expected behavior in vertical scaling scenarios, wasting your time, and creating confusion.

Now, when vertical load balancing is active and a machine reaches its session limit, it moves to a new state: “Maximum capacity for vertical scaling.” Director no longer generates alerts for this new

© 1997–2026 Citrix Systems, Inc. All rights reserved.

state. Alerts only trigger for “Maximum capacity” in horizontal scaling scenarios. You can view the new state in the **Filters** and **Custom reports** pages, making it easier to distinguish between expected and exceptional conditions. This enhancement helps you avoid unnecessary alerts and focus on real issues, streamlining monitoring and troubleshooting. It applies when you configure `UseVerticalScalingForRdsLaunches` using Set-BrokerSite and set the “Maximum number of sessions” policy in Studio.

Connector Appliance health alerts. Previously, creating and managing alerts for Connector Appliance was not available. With this release, you can create and manage alerts for Connector Appliance. This feature enables administrators to monitor the health of Connector Appliances using a single dashboard view and proactively configure alerts.

You can configure alerts under Advanced Alert Policies for the health/connectivity and resource utilization of Connector Appliances. Define severity and scopes for administrators to receive detailed alerts according to the alert configuration. For more information, see Connector Appliance health metrics.

Enhanced network metrics collection for session troubleshooting. Network metrics are critical for Citrix session troubleshooting because session performance and stability depend heavily on underlying network conditions. Unlike local applications, Citrix sessions stream interactive desktop or application experiences over a network, meaning any network instability directly impacts user performance.

Use the policies in Citrix Studio to enable or disable collection of specific network metrics based on your requirements. The policies provide Citrix administrators with granular controls to report metrics in adherence to compliance requirements. For more information, see Network metrics documentation.

Observability for multi-session VDA. The observability for multi-session VDA feature enhances the monitoring and troubleshooting capabilities for Secure Private Access sessions within a multi-user VDA environment. This feature empowers Citrix Helpdesk Administrators to monitor Secure Private Access sessions, troubleshoot issues, and gain insights into app launches and user transactions in case of a multi-session VDA.

Key features:

- Enhanced observability: Administrators can monitor Secure Private Access sessions, including app launches and enumerations, within the Citrix Director interface. This includes detailed views of enumeration and app launch issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- User context tracking: The feature maintains user context for apps accessed in a shared VDA environment, ensuring accurate session data visibility for each user.
- Error insights: Captures and displays Single Sign-On (SSO) failures, error codes (e.g., 6003, 6007), and troubleshooting steps to resolve issues.
- Session search: Administrators can search for sessions, apps, and user transactions using the same workflow as for VDI sessions and apps.
- Cross-session navigation: Enables navigation between Secure Private Access sessions and VDA sessions for streamlined troubleshooting.

For more information, see Observability for multi-session VDA.

Custom schedule for holidays. Autoscale™ now allows you to create custom schedules to turn off unused VMs in a delivery group on specific days, like holidays, to reduce unnecessary resource consumption.

To create custom schedules:

1. In Studio, go to **Delivery Groups**. Right click a delivery group and select **Manage Autoscale**.
2. On the **Schedule** page, click **Create schedule**.

For more information on creating custom schedules for holidays, see Create custom holiday schedules using Studio.

Support for Image Management with Azure Confidential VMs using Studio UI. You can now use the **Images** node to prepare and manage images that are compatible with Azure Confidential VMs. You can also use PowerShell commands to achieve this goal. For more information, see:

- Azure confidential VMs
- Create an image definition and initial image version

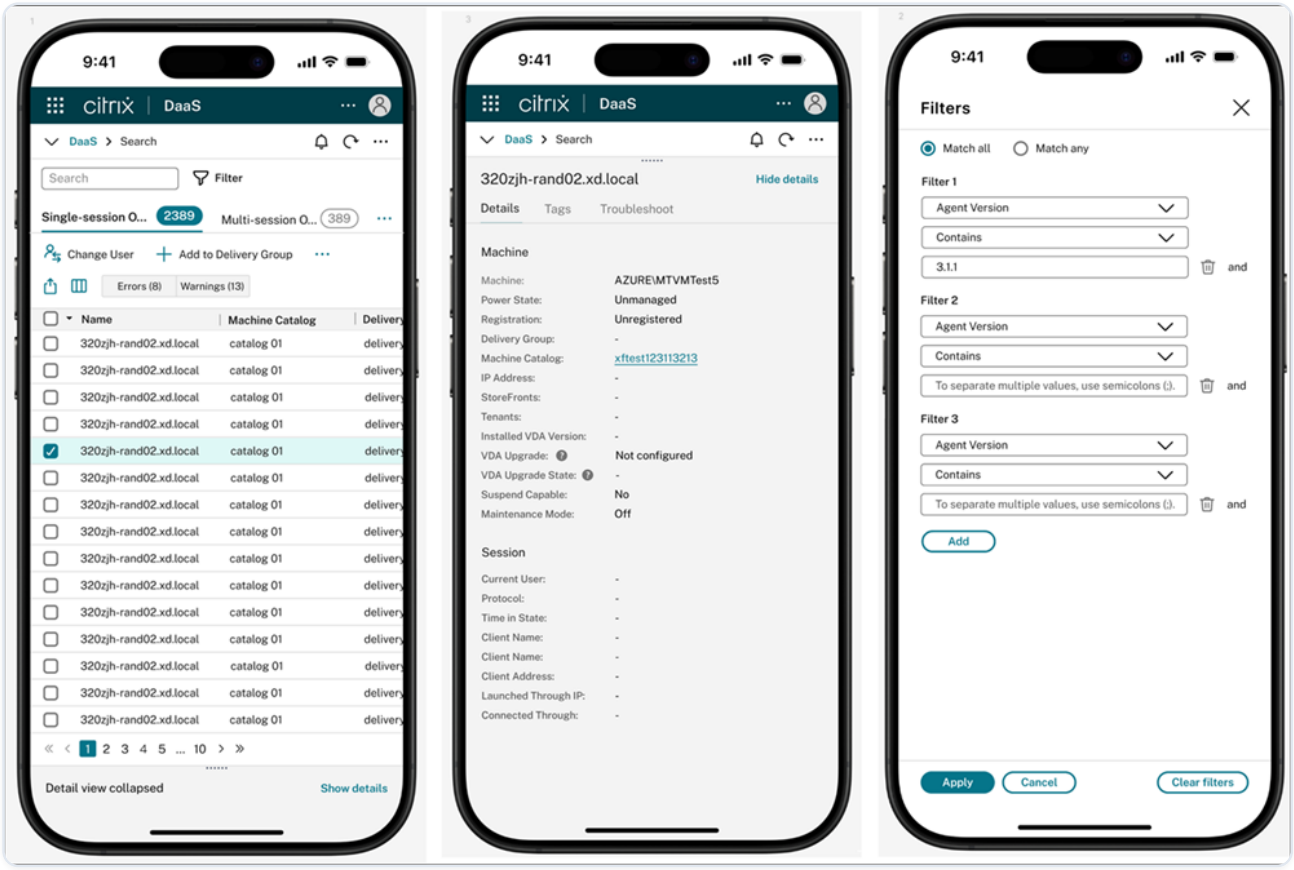
Enhanced mobile experience for critical on-the-go DaaS tasks. You can now manage Citrix DaaS more easily from your mobile device. The updated experience is optimized for smaller screens, making it easier to access Studio from a mobile device when a desktop isn't available. Whether you're responding to an alert or quickly checking a misconfiguration, you can take action right away—no need to wait until you're back at your desk.

The mobile interface offers improved accessibility and is designed for touch-friendly interactions. Layouts and functionality might differ slightly from the desktop experience to better suit mobile workflows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With a responsive layout and streamlined navigation, you can:

- Monitor DaaS health at a glance
- View details for machine catalogs and delivery groups
- Take key actions, such as restarting machines or disabling delivery groups



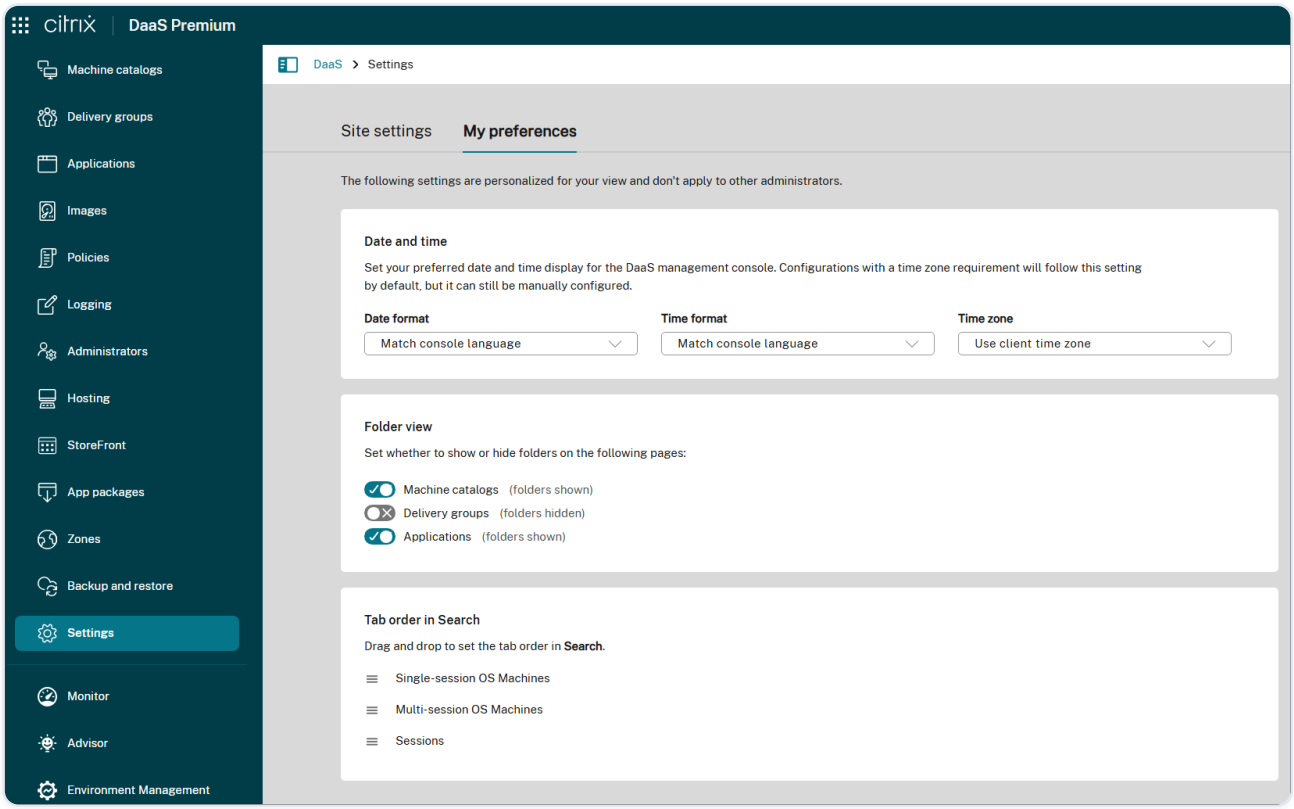
Customize your Studio view with My preferences settings. A new **My preferences** tab is now available under the **Settings** node. Settings on this tab let you tailor your Studio interface to suit your preferences. These settings apply only to your account and don't affect other administrators.

You can configure the following options:

- **Date and time**: Set your default time zone, date format, and time format. These settings are used throughout Studio for time-related displays, such as scheduled restarts and autoscaling.
- **Folder view:** Choose whether to show or hide the folder view in the **Machine Catalogs**, **Delivery Groups**, and **Applications** nodes.
- **Tab order in Search**: Customize the tab order within the **Search** node.

For more information, see Manage personal preferences in Studio

© 1997–2026 Citrix Systems, Inc. All rights reserved.

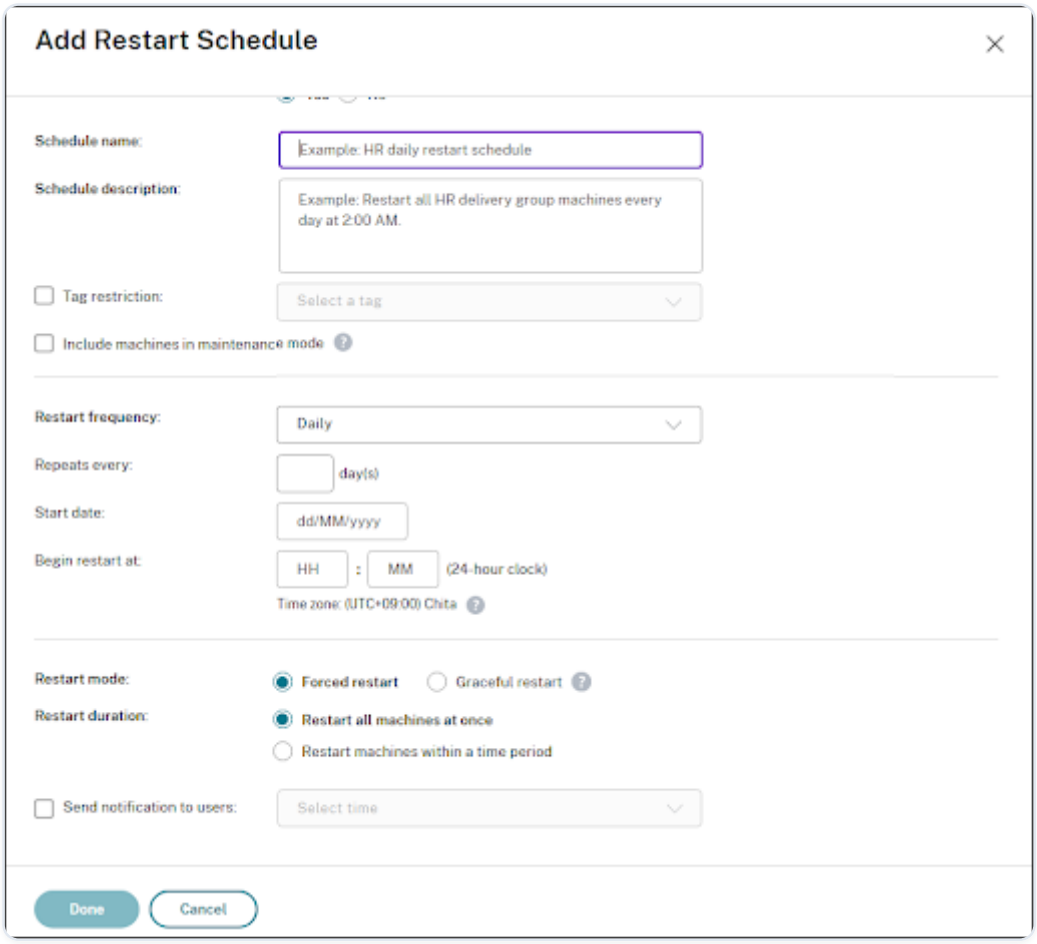


Improved restart UI for clearer control and customization. We've enhanced the restart schedule UI to make restart modes clearer and more customizable. You can now easily distinguish between *graceful restart* and *forced restart*, and configure custom restart durations to suit your needs.

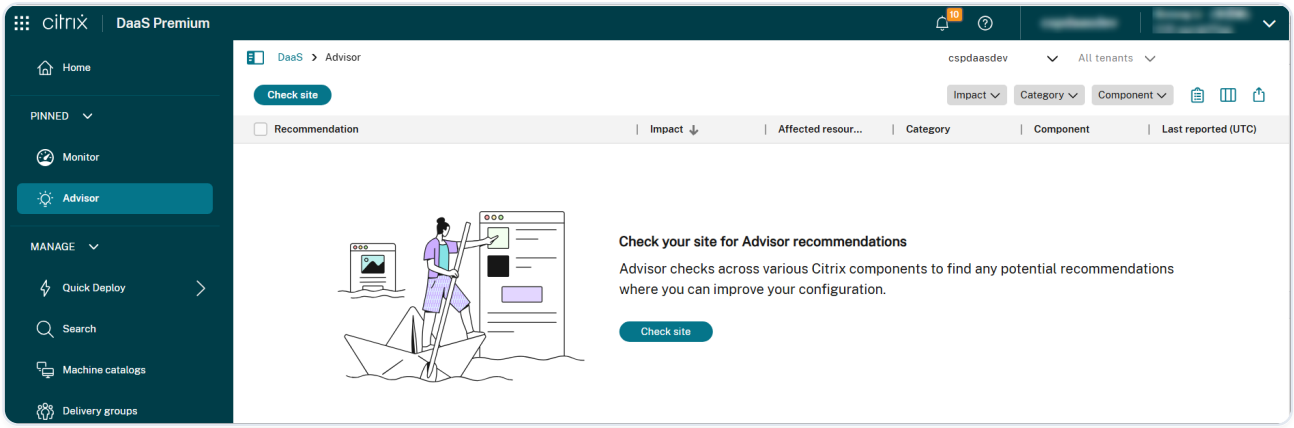
To help you make informed choices, we've also added tooltips that explain key options—such as how forced restart can forcibly restart machines, even if sessions are unresponsive.

For more information, see Manage delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix Advisor: Proactive insights and optimization for your DaaS deployment. Citrix Advisor is a service that helps you optimize DaaS deployment and enhance its overall health and readiness. It automates environment checks and delivers actionable recommendations, empowering you to proactively identify configuration issues, inefficiencies, resource wastes, deviations from best practices, and more.



With Advisor, you can:

- **Proactively identify and resolve issues:** Detect potential problems, configuration drift, and deviations from best practices before they impact users, disrupt business operations, or compromise security.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Optimize environment performance and stability:** Fine-tune configurations, optimize resource allocation, and implement best practices to enhance the stability, security, and performance of your Citrix deployments.
- **Streamline operations and reduce overhead:** Automate routine checks, simplify complex remediation tasks, and receive guided assistance, thus reducing operational overhead and freeing up administrative resources.
- **Optimize costs and resource utilization:** Identify areas of overspending, uncover opportunities for resource optimization, and ensure efficient utilization of Citrix technologies to minimize total cost of ownership.
- **Maintain compliance and adherence to best practices:** Ensure that Citrix deployments adhere to Citrix best practices, security standards, and industry regulations, reducing risk and improving overall governance.
- **Simplify complex tasks:** Simplify administrative tasks to support a healthy, optimized environment.

For more information, see Citrix Advisor.

July 2025

New and enhanced features

Cost summary. The **Cost summary** page provides a comprehensive summary of the expenses associated with running the Citrix environment. With this enhancement, you gain visibility into the following:

- The overall cost per user
- Cost of delivering virtualization by the chosen Workload providers, desktop types, and VM series sets

This page offers:

- Insight into the cost of delivering a virtualized app or desktop to a user The amount saved
- Information on costs and savings categorized by
  - Platform provider
  - OS type
  - Desktop type
  - VM series

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The **Cost summary** page is available only if the site has been running for at least 15 days in a month.

For more information, see the Cost summary page.

Cross-account provisioning in AWS EC2 using PowerShell. There are use-cases where the Cloud Connectors would like to be placed in a separate AWS account (shared services account or site components account) with IAM roles that have cross-account access (cross-account IAM role) and MCS-provisioned machine catalogs in separate secondary AWS account (workloads accounts), without the need for additional Cloud Connectors in the separate accounts. To support such scenarios, this feature uses VPC peering and cross-account access using IAM roles to make provisioning across different AWS accounts possible for enterprises managing multiple AWS accounts.

With VPC peering, you can have your Cloud Connector, and provisioned VMs in different regions or accounts be able to communicate among each other.

With cross-account access using IAM roles, you allow the primary account (Cloud Connector account) to assume an IAM role to access AWS resources in the secondary account (machine catalog VMs).

For detailed information, see Cross account provisioning.

Support for backup SKU list for VMs in AWS EC2. Public clouds can sometimes run out of capacity for a specific EC2 instance type (**Primary SKU**). If the primary VM configuration is not available, then the VM cannot start resulting in loss of time and business disruption.

With this feature, in the AWS virtualization environment, you can provide a list of backup EC2 instance types (**Backup SKUs** that can be **On-demand** instances) using PowerShell that MCS can fall back to in case of capacity-related issues. MCS tries to fall back on the backup EC2 instance types in the order that is provided by you in the list. In case MCS fails to fall back on all backup EC2 instance types provided, you get an error message. This feature is applicable to both persistent and non-persistent MCS machine catalogs.

For more information, see Backup SKU list for VMs.

Enhanced session launch diagnostics with recommended actions. The updated **Session Launch Failure Diagnostics** page offers a more thorough understanding of session launch issues. You can find the visualization of involved components with error analysis and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

recommended actions. Previously, only a **Transaction Details** panel was available, which listed involved components and indicated error locations.

The enhanced page now includes:

- Components overview: This section displays all components involved in the session launch process, adapting to the specific scenario and failure stage. Examples of components include Endpoint, Citrix Workspace™, Citrix DaaS, Cloud Connector, Gateway Service, VDA, and StoreFront. The root cause component is clearly highlighted.
- Error details: Specific error messages and context are provided for quick identification of the root cause.
- Transaction logs: Raw session launch event data is accessible for in-depth troubleshooting and analysis.

These enhancements enable IT administrators to resolve session launch issues more quickly and efficiently. For more information, see the Session Launch Diagnostics documentation.

Integration with Nutanix Prism Central on AHV. You can now connect Citrix DaaS to Nutanix AHV clusters through Nutanix Prism Central using a new host connection, Nutanix AHV Prism Central.

The benefits of using Nutanix AHV Prism Central host connection are:

- Supports machine catalogs with both power managed only and MCS provisioned VDAs.
- Enables MCS master VM sharing across AHV clusters using template version.
- Simplifies certificate trust on host connection.
- Eliminates the need to separately install the plug-in on Cloud Connectors.

For more information, see:

- Nutanix virtualization environments
- Nutanix cloud and partner solutions
- Connection to Nutanix
- Connection to Nutanix cloud and partner solutions
- Create a Nutanix catalog
- Manage a Nutanix catalog

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for creating non-persistent MCS machine catalogs in Amazon Workspaces Core. MCS has now integrated with Amazon Workspaces Core to provision non-persistent MCS machine catalogs in the customer's AWS account. For a comparison of how this new integration compares with MCS for AWS EC2 and Quick Deploy for Amazon WorkSpaces Core Bundles and how to set up the resource location, see AWS virtualization environments.

With this feature:

- You can create a host connection to Amazon WorkSpaces Core Managed Instances.
- Create a prepared image and use the prepared image and machine profile to create a non-persistent MCS machine catalog.

Customize desktop icons across platforms using Studio. Studio now allows you to customize desktop icons for any desktop of your choice. Previously, all desktops used the default icon, and you couldn't change it in Studio. You can now:

- Upload icons and use them for desktops or apps
- Change the icon for individual desktops
- Select from built-in icons for the desktops of your choice

For more information, see Create delivery groups and Manage delivery groups.

Studio: Support for more granular control over access policies in delivery groups. Previously, you could apply access policies to specific users only using PowerShell or REST APIs. Now, you can achieve this goal directly in Studio. This enhancement gives you more flexibility in defining different access conditions for various users or user groups, achieving more granular access control. For more information, see Configure user scope for an access policy.

Additionally, we've improved compatibility between Studio and the PowerShell or REST API approach. Previously, if you configured access policies with user scopes using PowerShell or REST APIs, the Users and Access Policies pages in Studio were blocked. Studio now fully supports these scenarios, offering clear information or UI guidance where necessary.

Option to use system proxy on Citrix Cloud™ Connectors for redirected Azure and GCP API traffic. With this feature, you can redirect Azure and GCP API internet traffic on Citrix Cloud Connectors through the system proxy. This helps you to route all external traffic through a non-transparent proxy.

For information on enabling the proxy, see:

- For Azure:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - Studio: Create a service principal and connection using Studio
  - PowerShell: Option to use system proxy on Citrix Cloud Connectors for redirected Azure API traffic

- For GCP:
  - Studio: Add a connection
  - PowerShell: Option to use system proxy on Citrix Cloud Connectors for redirected GCP traffic

Share encrypted prepared image across subscriptions and tenants for Azure. Azure Compute Gallery (ACG) images can be encrypted with a Disk Encryption Set (DES). With this feature, you can share an encrypted prepared image across subscriptions and tenants. You can thereafter create a machine catalog in the resource where the encrypted prepared image is shared. For more information, see Share encrypted prepared images across regions, subscriptions, tenants.

Add notes while assigning prepared images. With this feature, you can now add custom notes using Studio and PowerShell while creating or updating an MCS catalog with a prepared image. MCS keeps a record of all prepared image assignments. This helps you to:

- Retrieve the image assignments history of all the prepared images assigned to a catalog.
- Quickly roll back a machine catalog to a previously assigned prepared image using the **Use previous image assignment for quick rollback** action. Simply select a version from the history list for a quick and informed rollback. For information on rolling back, see Update a machine catalog with a different prepared image.

This feature is applicable to both Azure and VMware environments

For information on creating a catalog with prepared images, see:

- Create a prepared image machine catalog in Azure
- Create a prepared image machine catalog in VMware

For information on updating a catalog with prepared images, see Manage prepared image machine catalogs.

Support for Azure Arc onboarding across all on-premises hypervisor. Azure Arc enables organizations to manage resources such as VMs hosted anywhere as if they are running in Azure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With Azure Arc, you can use Azure services such as Azure Monitor for comprehensive visibility and proactive management of the resources.

With this feature, you can now enable Azure Arc Onboarding for an MCS machine catalog using PowerShell commands. Once onboarded, the VMs can be managed from the Azure portal to perform operations such as power management, add or remove extensions, assign policies, and enable Azure Monitor on the Arc-enabled VMs through built-in Azure policy.

Currently, this feature is applicable to all Citrix on-premises hypervisors Vmware, Nutanix and SCVMM.

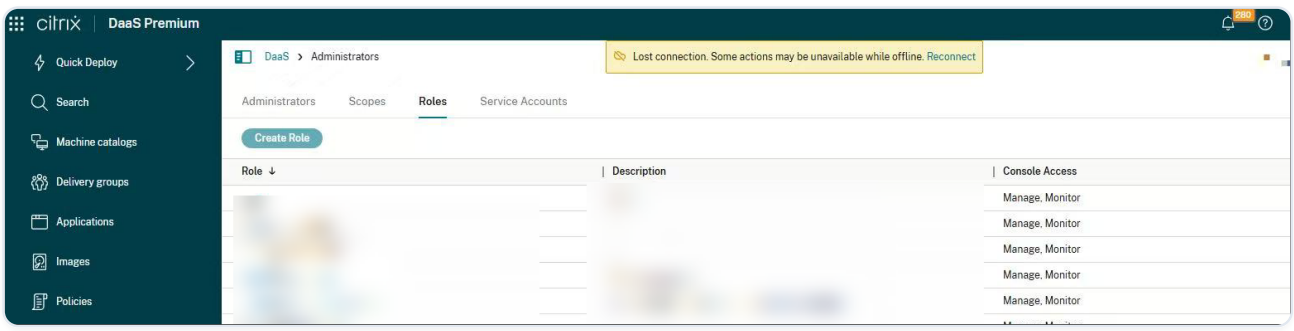
For more information, see Onboard VMs to Azure Arc.

Migration from unmanaged to managed disks in Azure. On September 30, 2025, Azure will officially retire unmanaged disks (that is, VHDs). After this date, you will no longer be able to start Azure VMs that use unmanaged disks. With this feature, you can migrate your MCS-provisioned Azure VMs from unmanaged to managed disks through Citrix.

The migration applies to both persistent and non-persistent machine catalogs, supporting both on-demand and legacy VMs. This ensures seamless integration with Azure's updated disk management standards and prevents any service disruptions due to the retirement of unmanaged disks. For more information, see Migrate from unmanaged to managed disks.

Support for Image Management with Azure Confidential VMs. You can now prepare and manage images that are compatible with Azure Confidential VMs. These images ensure that VMs provisioned from such MCS machine catalogs are encrypted in memory and protected while in use. For more information on Image Management, see Image management.

Studio always-on mode. Web Studio now introduces always-on mode to enhance resiliency and reduce downtime during infrastructure failures. In this read-only mode, you can securely view and monitor your Citrix DaaS environment even during service disruptions, helping maintain operational continuity. Always-on mode is available on all MANAGE nodes, except Quick Deploy. For more information, see this blog post.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Studio: Support for managing Azure AD security groups using service accounts. In Studio, you can now use Azure AD service accounts to configure and manage dynamic security groups for VMs. Previously, configuring Azure AD security groups required manually entering credentials. This update allows you to use a pre-configured service account to perform security group management without user interaction, simplifying the process and enhancing security.

For more information, see Azure AD service accounts and Create a Microsoft Azure catalog.

Migrate existing MCS provisioned catalogs to prepared image machine catalog. With this feature, you can convert an existing MCS catalog provisioned from master image to a catalog using a prepared image. For information on prepared image, see Image management.

However, you cannot revert to the legacy catalog after migration. Currently, this feature is applicable to Azure and VMware virtualization environments. For information on the steps to migrate, see Migrate existing MCS provisioned catalogs to prepared image machine catalog.

Display NVMe v6 SKUs for ephemeral OSDisk usage. You now have the option to store an ephemeral OS disk on a NVMe Disk using Studio. For information see, Azure ephemeral disks.

Updated duration of Pending HA state. The Pending HA state duration when Cloud Connectors determine if there is a need to enter LHC mode has been extended from 60 to 90 seconds. For information on LHC states, see Local Host Cache states.

June 2025

New and enhanced features

Support for assigning Citrix Group Policies to Microsoft Entra ID users. You can now assign Citrix Group Policies to Microsoft Entra ID (Azure AD) users from multiple IDPs in Studio. This enhancement gives you more flexibility when applying policies to specific user groups and simplifies deployments using Citrix DaaS with Windows 365. For more information, see Specify policy assignments.

Monitoring VDA logon duration details. Citrix Monitor now includes detailed information on VDA logon duration to provide visibility into the time taken to log on to the VDA. The following items are added to view the details of VDA logon duration:

- The following metrics are added to the tooltip as breakdown metrics:
  - **AppX file associations**: The time taken to associate AppX files during the new VDA session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **AppX load packages**: The time taken to load the AppX packages during the new VDA session.

  These metrics are exported in PDF and CSV formats, and the chart is also included in the exported files.

- Breakdown of **Shell** step on the **Session Logon** tab: AppX file associations and AppX load packages are added as a breakdown of interactive session step on the graph on the **Session Logon** graph tab.

Benefits:

- Accurate troubleshooting: Helps administrators accurately determine the causes of slow logons, which might be often due to deployment type, GPOs, profiles, and user interaction.
- Corrective actions: Enables administrators to take corrective actions in the right areas, improving the overall user experience.

This feature is designed to improve the session logon breakdown, providing a more accurate representation of logon performance and session logon triage for the Director help desk.

For more information, see Logon process phases.

Endpoint metrics available on the Filters tab and Custom Reports. Previously, endpoint metrics were available only in the Endpoint view at the **User Details** > **Session Performance** > **Session Topology** section.

With this enhancement, you can now view the following more endpoint metrics in the Monitor Connection or Session filters and Custom Reports:

- Public IP address
- ISP
- Location (Country or City)
- Workspace type - Citrix Workspace app (app or browser)
- Access type (through Workspace or StoreFront)

This enhancement helps you to do the following:

- You can select the endpoint metrics as part of column selection in the **Filters** tab.
- You can create custom reports using the **Custom Query** option by selecting output columns as endpoint metrics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bulk alert dismissal. This feature aims to optimize the alert management process for administrators by providing more flexibility and reducing alert fatigue. It allows administrators to bulk dismiss alerts by time, type or category, making it easier to manage alerts, especially during maintenance modes or when dealing with alerts from hypervisors and other environments.

By allowing bulk dismissal of alerts, administrators can manage their workload more efficiently and avoid being overwhelmed by a high volume of alerts.

For more information, see Bulk alert dismissal.

Enhanced network metrics monitoring in Citrix Monitor. Citrix Monitor now provides administrators with unparalleled visibility into session performance. This enhancement empowers them to proactively identify and address bottlenecks, optimize applications, and ensure a superior user experience.

Key enhancements:

- **L7 latency monitoring**: Pinpoint and resolve performance issues by monitoring application-level processing time (L7 latency).
- **New network metrics**: Gain a comprehensive understanding of network performance through insights into throughput and client-side retransmits.
- **Historical data**: Identify patterns and potential issues by viewing latency trends for the past 15 minutes and 24 hours.
- **Filtering**: Perform targeted analysis and troubleshooting by filtering latency data in the **Filters** page.
- **Session connection path visualization**: Quickly identify and resolve latency issues by visualizing the end user's connection path to VDA machines, including network hops and components.

Benefits:

- **Enhanced visibility**: Rapidly identify the root causes of poor in-session experiences.
- **Efficient troubleshooting**: Streamline latency troubleshooting with a clear visualization of the session connection path.

Metrics collected:

- Throughput
- L7 Server Latency

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L7 Client Latency
- Client-Side Retransmits

NOTE:

- To view the new metrics, enable the **Network Telemetry** policy in Citrix Web Studio. After enabling the policy, users must launch a new session for the changes to take effect.
- L7 latency is measured for HDX™ sessions established with Citrix Workspace app for Windows and Windows VDA through the Gatxeway service.
- After launching a session:
- New metrics are available in the **Session Topology** and **Last 15 Minutes** sections after a 2-minute wait.
- Historical data (from the last 48 hours) is available after approximately 5 minutes due to the 5-minute aggregation window.

With these enhancements, Citrix Monitor equips administrators with the tools to proactively optimize application performance and deliver a seamless user experience.

For more information, see End-to-end Network Hop view documentation.

Support for Citrix-managed OpenShift plug-in. With this feature, Citrix manages your Red Hat OpenShift workloads through a Citrix-managed OpenShift plug-in. With this plug-in, you can create hosting connections and hosting units to your OpenShift cluster, create catalogs, and power manage machines in the catalog. For more information, see:

- Red Hat OpenShift virtualization environments
- Connection to Red Hat OpenShift
- Create a Red Hat OpenShift catalog

Improved UI performance for importing VMs from AWS. We've enhanced Studio UI performance by optimizing the process of importing VMs into Citrix DaaS from AWS. To prevent timeouts caused by fetching a large number of AMIs, Studio no longer retrieves AMIs during this process.

Service account for routing Azure AD Identity traffic. Using this feature, you can create and modify an Azure AD service account to route Azure AD identity traffic from Delivery Controller to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure AD through Citrix Cloud Connector to enhance security. For more information, see Route Azure AD device management and security group management traffic.

Support for assigning security groups per network interface to VMs using the machine profile in AWS. In the AWS virtualization environment, you can now create an MCS machine catalog where the provisioned VMs are assigned security groups per ENI (Network Interface). To do this, use a machine profile input (EC2 instance or launch template) that has different security groups mapped to distinct ENIs. For example, if machine profile input has ENI A with SG 1 and ENI B with SG 2, then provisioned VMs will also have ENI A with SG 1 and ENI B with SG 2.

This feature applies to:

- Persistent and non-persistent catalogs
- New machine catalogs
- New VMs provisioned to an existing catalog

For information, see Create a machine profile-based machine catalog using PowerShell.

Support for creating host connections using Azure Managed Identity using Studio. Using Studio, you can now create host connections to Microsoft Azure Resource Manager using Azure Managed Identity. This method offers a secure and scalable alternative to using a service principal, eliminating the need to manage credentials manually. Managed identities support automatic token refresh and reduce the risks associated with storing and rotating secrets. Alternatively, you can use PowerShell. For more information, see Create a host connection using Azure Managed Identity and Manage Azure Managed Identity of an existing hosting connection.

Cost modeling for Azure workloads. The new cost modeling feature supports Azure workloads and provides recommendations based on usage patterns. Customers receive recommendations on whether Azure Reservations or Savings Plan is more suitable to provide maximum cost savings. Azure Reservations customers reserve a specific number of machines upfront at a discounted flat cost, while savings plans allow them to commit to a dollar amount for discounted rates. The feature analyzes the last 28 days of data to provide estimated recommendations. This feature helps customers save costs by making informed decisions on resource allocation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For optimal estimates, it is recommended to use data from a stable environment over the last 28 days. Avoid using data from periods of unusual activity, such as vacations or sudden spikes in usage. Wait until your usage returns to baseline levels before taking these recommendations.

Benefits:

- Provides tailored cost-saving recommendations.
- Supports both reservation and savings plans.
- Analyzes recent usage data for accurate insights.
- Helps optimize resource allocation and reduce expenses.
- Offers flexibility in selecting delivery groups, tags, VM series, and regions.

For more information, see the Cost modeling page.

View and filter machines by VDA upgrade state in Studio. Studio now includes **VDA Upgrade State** as a column in the **Search** and **Machine Catalogs** nodes. This column shows the status of scheduled VDA upgrades—for example, whether an upgrade was successful. You can also filter machines based on their VDA upgrade state, making it easier to track and manage VDA upgrades across your deployment.

For more information about this column, see Machine actions and columns.

Option to extend monitoring of HDX optimization beyond Microsoft Teams. Citrix Monitor now adds an option to extend the monitoring of HDX optimization beyond Microsoft Teams. Previously, only Microsoft Teams was available for monitoring HDX optimization, showing whether it was optimized or not in the **Session Topology** screen. With this new feature, instead of **Microsoft Teams**, a new parameter called **Real-time communications** is added on the **Session Topology** screen. Currently, only Microsoft Teams is monitored for HDX optimization status. However, this feature provides the possibility of adding more software for monitoring beyond just Microsoft Teams in the future. This feature allows administrators to monitor and troubleshoot applications with and without HDX optimizations, providing a better user experience.

You can click **View details** next to the application to view additional information, such as categorization under Third-Party Optimization and HDX Optimization. For Microsoft Teams Slims

© 1997–2026 Citrix Systems, Inc. All rights reserved.

core, it is part of third-party optimization. If not part of third-party optimization, then it is HDX optimized.

Key features and benefits:

- **Comprehensive monitoring**: Monitor and troubleshoot both HDX optimized and non-optimized applications.
- **Detailed insights**: View detailed information about the optimization status of applications.

NOTE:

- To use this new feature, ensure that you are using the Citrix Workspace app for Windows version 2503 and VDA version 2503.
- For using Microsoft Teams Slims core, you must install the Plug-in manager on the endpoint, configure the allow list for the virtual channel, and ensure that the virtual channel is open. This feature is only for HDX sessions.

For more information, see HDX optimization details.

New metrics in the Monitor dashboard. Citrix Monitor dashboard is enriched with the following two metrics to provide valuable insights for administrators:

- **Total connected users**: Shows the number of users who had at least one connection in the last 24 hours and the last 7 days. Helps the admins to showcase adoption trends to their executives.
- **Citrix Workspace app versions found in your environment**: Provides an overview of the Citrix Workspace app versions used across the organization. It helps in unifying the versions by showing how many devices are using different versions. You can select the **All** or specific OS from the **Platform** drop-down list.

This feature provides essential data points for administrators to monitor and manage their environments effectively.

Fore more information, see Site Analytics page.

Enhancements to Cost savings page. The following enhancements have been made to the Cost saving page to provide you greater flexibility and insight when managing costs:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Service provider filter supportability option**: You can now filter by service providers. If a site has both cloud and on-premises workloads, you can now filter by all cloud providers, all on-premises providers, or individual providers.

  NOTE:

  The filter is applied immediately upon selection without an apply button.

- **Multiple delivery group selection**: Previously, you can only select a single delivery group (DG) or all DGs. Now, you can select up to 15 DGs at once. If a site has fewer than 15 DGs, you can select all available DGs. You can also exclude specific DGs from the selection to view data for the remaining DGs.
- **Insight into failed machines**: The **Cost savings** page now provides visibility into machines in a failed or unregistered state. The following two new fields are included:
  - **Failed state with no sessions**: This field displays the count of machines that are in a failed state and have no active sessions.
  - **Unregistered with sessions**: This field displays the count of machines that are in an unregistered state but still have active sessions.

You can see the count of machines in the preceding states and act based on the failure reason, time, and delivery group. The counts are clickable links that navigate to the **Filters** page for further actions. The count includes both single-session and multi-session machines.

NOTE:

Filters are preserved across page navigation.

For more information, see the Cost savings page.

May 2025

New and enhanced features

Share encrypted prepared image across regions in Azure. Azure Compute Gallery (ACG) images can be encrypted with a Disk Encryption Set (DES). With this feature, you can share an encrypted prepared ACG image across multiple regions in the same subscription and tenant using

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DES. You can thereafter create a machine catalog in the region where the encrypted prepared image is shared. For more information, see Share encrypted prepared image across regions.

Update properties of individual VMs in VMware. You can now update properties of individual VMs in a persistent MCS machine catalog using a PowerShell command. This implementation helps you to manage individual VMs efficiently without updating the entire machine catalog. Currently, this feature is applicable only to the Azure and VMware virtualization environments. For more information, see Update properties of individual VMs.

Support for updating MCS provisioned machines in VMware environments. In VMware environments, `Set-ProvScheme` changes the provisioning scheme and does not affect existing machines of an MCS machine catalog. Using the PowerShell command `Set-ProvVMUpdateTimeWindow`, you can now apply the current provisioning scheme to an existing persistent or non-persistent machine or set of machines. This feature is applicable to machine profile and non-machine profile-based machine catalog. For more information, see Update provisioned VMs to current provisioning scheme state.

Estimate Azure VM costs during catalog creation. When creating a machine catalog, you can now estimate the monthly cost of Azure virtual machines, including VM size and disk costs. You can also refine the estimate by adjusting settings such as daily power-on hours, workdays, savings plans, reserved instances, and shutdown storage. This feature helps you plan deployments more efficiently and optimize costs early on.

For more information, see View monthly estimate details.

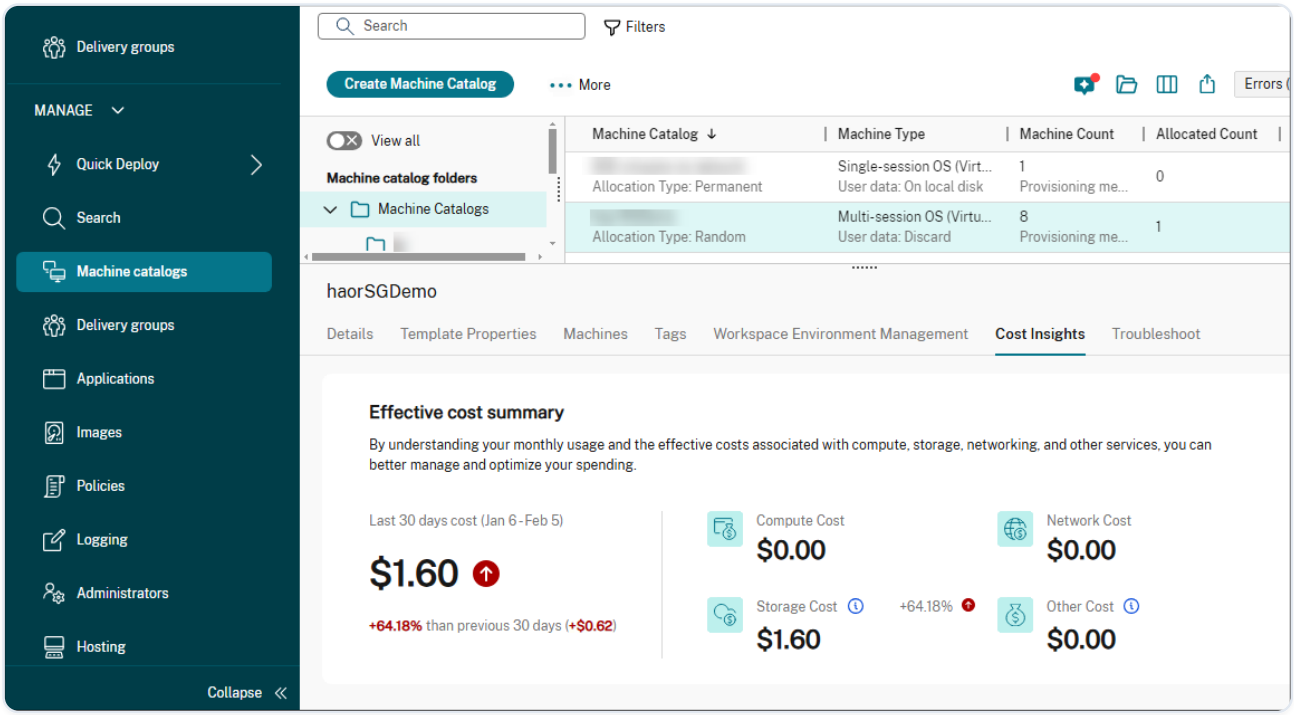
Visualization of provisioning cost insights. You can now view detailed cost information for machine catalogs. The visualization provides an overview of provisioning costs and trends for the last 30 days.

The report breaks down provisioning costs based on individual catalogs, allowing for a clear understanding of how each category contributes to the overall cost. The report:

- Displays the total cost incurred over the past 30 days.
- Compares the current 30-day total cost with the previous 30-day period.
- Displays cost details of:
  - Compute cost
  - Storage cost
  - Network cost

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Other cost



For more information, see View catalog details.

Support for converting machine catalogs from using master images to using prepared images. With a new action, **Convert to Prepared Image**, in Studio, you can now convert MCS-provisioned machine catalogs using master images to catalogs using prepared images. The converted catalogs cannot be reversed. This feature is available for Azure and VMware virtualization environments.

For more information, see Convert MCS-provisioned catalogs from using master images to using prepared images.

Proxy configuration for service accounts. Service accounts creation now supports proxy configuration through NGS Proxy for Azure AD Identity management. With this feature, you can:

- Delete Azure AD devices for Azure AD joined catalogs
- Delete Intune devices for Azure AD joined and Intune enrolled catalogs
- Create, edit, and delete Azure AD security groups

For more information, see Create an Azure AD service account.

Connector Appliance health metrics. The **Connector Appliance** component is added by default as part of Infrastructure monitoring. The **Connector Appliance** component that is connected to the Citrix DaaS site is auto onboarded for monitoring.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature enables customers to monitor Connector Appliance's health under the Infrastructure monitoring dashboard.

You can select the required **Component** type and the details are displayed according to the selected site name. You can also select the **Resource location**. For more information, see Connector Appliance health metrics.

April 2025

New and enhanced features

Use Autoscale to hibernate VMs. The power management is now enhanced to support hibernation of VMs through Autoscale configurable settings. Use the PowerShell commands `Get-BrokerDesktopGroups`, `New-BrokerDesktopGroups`, or `Set-BrokerDesktopGroups` to set the following positive value to the parameter `AutoscaleScaleDownActionDuringPeak` (during peak) or `AutoscaleScaleDownActionDuringOffPeak` (during off peak) to define the power actions:

- 0: Shut down the VMs when scaling down
- 1: Suspend (hibernate the VMs) when scaling down

VMs not capable of hibernation are shut down.

Intelligent Autoscale. Intelligent Autoscale is a data driven Autoscale feature with minimum administrative settings that allows you to configure the performance target of a delivery group. The performance target value ranges from 1 to 99 and the value specifies a target balance between user experience and cost:

- A low value prioritizes cost savings.
- A high value prioritizes user experience.

The performance target, combined with historical usage data, calculates an optimal buffer capacity (the number of VMs to be powered on) for each 30-minute block of a day. Therefore, 48 optimal buffer capacities are computed at the start of each day.

The optimal buffer capacity replaces peak and off-peak buffer capacity and pool size to manage available machines.

For more information, see Intelligent Autoscale schedules plugin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Studio: Support for exercising access control over apps at the delivery group level. Previously, within Studio, you could only exercise access control over apps at the individual app level, not at the delivery group level. Now, you can perform access control over apps at the delivery group level. Currently, this ability is limited to controlling access to all apps within a delivery group. For more information, see Restrict application access to specific users.

Client Platform filter for policy assignments. You can now control policy assignments more precisely with a new filter, Client Platform. This filter lets you assign (Allow) or exclude (Deny) policies based on the operating system of users' devices, including Windows, macOS, Linux, iOS, Android, or HTML5. This enhancement offers greater flexibility and precision in policy assignment, ensuring a customized and uniform experience across managed and unmanaged devices. For more information, see Policy assignments.

Option to reset In-Use Active Directory (AD) accounts. With Studio you can now reset machine Active Directory (AD) accounts even when the status of the machine is In Use. This enhancement is necessary because sometimes the system doesn't correctly detect when a machine is in a *tainted* state.

Support for provisioning Data disk in VMware. A Data disk allows storage of persistent data like event logs, security traces, and application data. With this feature, you can now create and assign a persistent and non-persistent Data disk to an MCS created persistent or non-persistent VM of an MCS machine catalog in VMware.

The Data disk must be provisioned from the master image. The provisioned VM's Data disk derives properties like storage policy, size, and so on from the master image. For machine profile based catalog, it can optionally use the VM template’s Data disk for deriving the properties. If the VM template doesn't have a data disk, then Storage's default policy is used. For information on creating an MCS machine catalog with a Data disk, see Provision a Data disk on MCS created VM.

Enable trusted launch of existing persistent and non-persistent catalogs. With this feature, you can update an existing non-Trusted Launch persistent and non-persistent machine catalog to a catalog enabled with Trusted Launch.

To successfully create or update a machine catalog with Trusted Launch, you must use a machine profile. However, if you use a master image enabled with Trusted Launch and a machine profile not enabled with Trusted Launch, you get a warning message because of the mismatched Trusted Launch configuration between master image and machine profile.

For more information, see Machine catalogs with trusted launch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Simplified Azure AD security group management using service accounts. Previously, managing the Azure AD security group required you to log in to Azure AD and get the access token.

With this enhancement, MCS now supports using a pre-created service account to manage Azure AD security groups for Azure AD joined machines. However, to use a service account with Azure AD security group management capability, you need some permissions. For information, see Permissions required for an Azure AD service principal.

You can use the service account to do the following without the requirement to get the access token.

- Create a machine catalog with Azure AD dynamic security group
- Enable security group feature for an Azure AD catalog
- Delete a machine catalog with Azure AD joined device security group
- Create an Azure AD dynamic security group under an existing Azure AD assigned security group

For information, see:

- Azure Active Directory dynamic security group
- Create an Azure AD dynamic security group under an existing Azure AD assigned security group

Support for creating Hybrid Azure AD joined catalogs and Hybrid Azure AD joined catalogs enrolled in Microsoft Intune with prepared images. With this feature, you can now use prepared images to create Hybrid Azure AD joined catalogs and Hybrid Azure AD joined catalogs enrolled in Microsoft Intune using Studio and PowerShell commands. This feature is applicable to single and multi-session persistent and non-persistent type MCS catalogs. However, currently, you can create catalogs for Hybrid Azure AD joined catalogs enrolled in Microsoft Intune for only persistent single and multi-session VMs. Enrollment of Hybrid Azure AD joined non-persistent VMs into Microsoft Intune is currently under preview.

This implementation significantly reduces the storage and time costs, and simplifies the VM deployment and image update process. For the complete set of Powershell commands to create image definition, image version, and prepared image version spec, see Use PowerShell. For information on creating a Hybrid Azure AD joined catalog and Hybrid Azure AD joined catalogs enrolled in Microsoft Intune, see Identity pool of Hybrid Azure Active Directory joined machine identity and Create Hybrid Azure AD joined catalogs enrolled in Microsoft Intune.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for SCVMM 2025. Citrix DaaS now supports Microsoft's System Center Virtual Machine Manager (SCVMM) 2025. SCVMM provides a range of services to include maintaining the resources you need to deploy VMs. For more information about the new features supported in SCVMM 2025, see What's new in System Center Virtual Machine Manager.

Support for automatically using Azure Temporary Disk for write-back cache disk. When you edit an MCS-provisioned catalog in Studio, the catalog now automatically uses Azure Temporary Disk for the write-back cache (WBC) disk if the required criteria are met. As a result, new VMs added to the catalog uses Azure Temporary Disk for the WBC disk.

Previously, if a catalog didn't qualify at creation, Azure Temp Disk wasn't used for WBC disk—even if the catalog was later updated to meet the criteria.

Benefits:

- Reduce costs. Temp Disks don't incur storage costs when the VM is powered off.
- Improve flexibility. Use Temp Disks for WBC without recreating the catalog.

An MCS-provisioned catalog automatically uses Azure Temp Disk for WBC disk when the catalog meets all the following criteria:

- MCSIO is enabled.
- The WBC disk is non-persistent.
- The VM size includes a Temp Disk large enough for the WBC disk.
- No drive letter is specified for the WBC disk.

For more information, see Create a Microsoft Azure catalog.

App visibility control support for Azure AD users. Previously available only for Active Directory users, the ability to restrict app visibility is now extended to Azure AD users. With Studio, you can now control which Azure AD users and groups can see a specific app in the Workspace app.

This function requires VDA version 2411 or later. For more information about detailed steps, see Change application properties > Limit visibility.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

March 2025

New and enhanced features

Re-trust option for untrusted host connection certificates. If a host connection outage occurs due to an untrusted certificate, you can re-trust the certificate for that host connection in Studio. For more information, see Test TLS Certificate Trust.

Re-sync deployments in AWS UI. A new option to re-sync deployments in AWS is added. Re-sync a deployment that is in Pending state or if the number of machines listed in a deployment does not match with the number of machines listed in AWS.

NOTE:

- When a deployment of Active or Error state is re-syncing, the status of that deployment changes to **Syncing machines**.
- When a deployment of Pending state is re-syncing, the status continues to show as **Pending** until completed.

For more informantion, see Create a deployment.

Centralized site management is generally available. As a Cloud Administrator of multiple sites, you can now designate one site as the primary and link other sites to it for streamlined, centralized management. This feature helps improve operational efficiency by reducing the need to switch between sites for daily tasks.

Key benefits:

- **Efficient site management**: Administrators can manage multiple sites from a single interface, switching between them using the drop-down menu in the upper-right corner, eliminating the need to change accounts.
- **Seamless navigation**: Administrators can seamlessly switch between Studio and Monitor without needing to reselect the site. When a site is selected in Studio, it's automatically selected in Monitor, streamlining your workflow.
- **Simplified help desk operations**: Help desk administrators can view information for all sites in one Monitor console.
- **Aggregated end-user experience**: End users sign in to a single Citrix Workspace URL (for example, customer.cloud.com) to access resources from linked sites.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Centralized site management.

UI Enhancements in Studio. Web Studio introduces the following improvements to enhance your administration efficiency:

- Copying data from tables

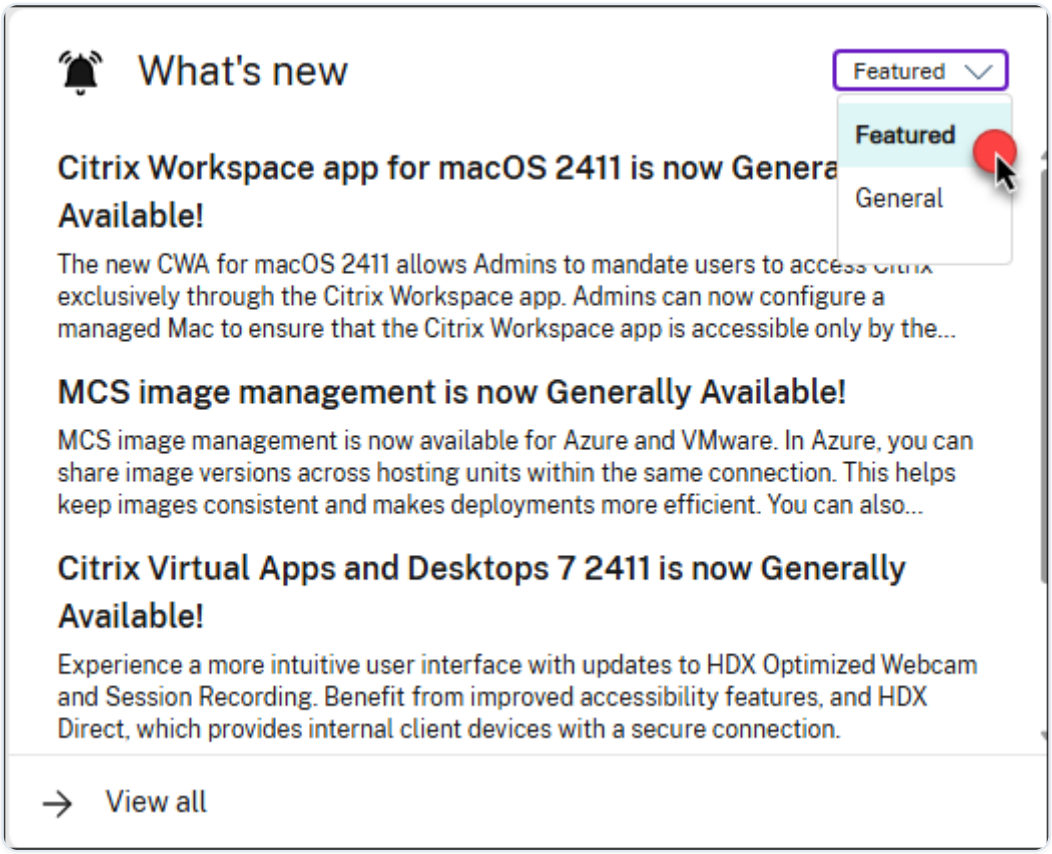
  You can now copy data directly from table components, such as "Machine name" on the Machine Allocation table. This enhancement reduces the need for manual data entry, minimizing the risk of errors.

- Pagination for tables

  Table components now support pagination, boosting performance and usability.

What's new widget enhancement. A new feature has been introduced to the What's new widget on the Studio **Home** page. You can now seamlessly switch between two content sources:

- **Featured**: Curated, handpicked content for quick product insights and highlights.
- **General**: A comprehensive list of content sourced directly from the DaaS documentation for in-depth, extensive feature updates. This update ensures that you have the flexibility to access both curated and extensive content, enhancing your experience and keeping you well-informed.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Token usage limit in token-based enrollment increased to 5000. We've increased the token usage limit in token-based enrollment from 100 to 5000, allowing for greater flexibility when enrolling machines in large-capacity machine catalogs.

For more information, see Generate and manage enrollment tokens.

Migration of non-persistent VMs in VMware. Previously, in the VMware environment, you could migrate only the persistent VM disks from one storage to another storage. With this feature, you can migrate the non-persistent VM disks from one storage to another storage using the `Move-ProvVMDisk` PowerShell command. You can migrate: OS Disk, Identity Disk, and Write-back Cache (WBC) disk.

For more information, see Storage migration of VMs.

Migration of persistent and non-persistent VMs in XenServer®. With this feature, in the XenServer environment, you can migrate the following VM disks from one storage to another storage using the `Move-ProvVMDisk` PowerShell command.

- For persistent full clone VMs: OS Disk, Identity Disk, and non-MCS provisioned disks.
- For non-persistent VMs: OS Disk, Identity Disk, and Write-back Cache (WBC) disk.

For more information, see Storage migration of VMs.

Enhanced Autoscale features for improved power management. We've enhanced Autoscale to improve your experiences. You can now:

- Receive notifications if machines in a delivery group don't support hibernation, along with recommendations for alternative actions, such as shutting down those machines.
- Choose to suspend machines over stopping them, wherever supported.
- Set restart schedules for suspended machines to prevent them from remaining suspended indefinitely.

For more information, see Schedule-based settings and Load-based settings.

Improvement to Workload rightsizing. The **Workload rightsizing** (formerly Infrastructure Rightsizing) tab now includes an option to identify power users. This feature allows you to export the details of power users.

NOTE:

This feature is available only for single-session OS delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Export** data includes **User Name**, **Total Session Count**, **Average Session Duration (Mins)**, **Peak CPU Usage (%)**, and **Peak Memory Usage (%)**.

This enhancement provides valuable insights into resource utilization and helps in optimizing infrastructure costs by ensuring efficient resource allocation based on user behavior. For more information, see Workload rightsizing page.

Enhancement to Session Performance tab. The **Session Topology** section of the **Session Performance** tab is enhanced to include the following:

- **Protocol**: Displays the MTU value for EDT protocol. For example:
  - Single-stream: EDT (MTU = 1500)
  - Multi-stream: EDT (MTU stream IDs 0=1500, 1=1500)
- **MS Teams**: Displays whether HDX optimized or not HDX optimized.
- **HDX Connection Type**: Displays the HDX connection type. For example: HDX, HDX Direct, and Rendezvous.
- **Frames Per Second** provides information on:
  - Input Frames Per Second
  - Output Frames Per Second

Security groups configurations are inherited from machine profiles. You can now create an MCS machine catalog and select a machine profile that has security groups assigned. This avoids the security group configuration as it is inherited from the machine profile. Alternatively, if you do not select a machine profile, at the time of MCS machine catalog creation then configure the security groups in the Security page in Studio. For more information, see Security.

Autoscale holiday plug-in. With this feature, you can deviate from the standard Autoscale settings related to the power management of VMs and allow VMs to be powered off on specified holiday dates. For example, for weekdays you want most of the VMs to be powered on and by default, on public holidays, the weekday schedule is applied. To manage such scenarios, use the Autoscale holiday plug-in to power off the VMs on specified holiday dates.

For more information, see Autoscale holiday plugin.

Match UEFI boot program to Citrix Provisioning version for MCS created Citrix Provisioning catalogs. The Citrix Provisioning server uses a BDM disk, which contains a UEFI boot program. This feature allows generation of `BOOTX64.EFI` file alongside the `PVSBOOT.INI` file when

© 1997–2026 Citrix Systems, Inc. All rights reserved.

creating a Citrix Provisioning catalog using MCS. As a result, target devices can boot from the latest boot settings file, ensuring that target devices align with the Citrix Provisioning version.

Support for creating Azure AD joined and Microsoft Intune enrolled catalogs with prepared images. With this feature, you can now use prepared images to create Azure Active Directory joined and Microsoft Intune enrolled catalogs using Studio and PowerShell commands. This feature is applicable to single and multi-session persistent and non-persistent type MCS catalogs. This implementation significantly reduces the storage and time costs, and simplifies the VM deployment and image update process. For the complete set of Powershell commands to create image definition, image version, and prepared image version spec, see Use PowerShell. For information on creating an Azure AD joined catalog and Azure AD catalog enrolled in Microsoft Intune, see Identity pool of Azure Active Directory joined machine identity and Create Azure AD catalogs enrolled in Microsoft Intune.

Flexible storage location option for VMs. Previously, VM allocation began from a fixed Storage Service (SR), such as SR1, and progressed sequentially through SR2, SR3, and so on. And, for some cases, the storage load is not evenly distributed across storages.

This feature gives you the ability to balance VM allocation across different storage service using the following methods:

- **Enhanced current round robin allocation method**: Instead of always starting from the same fixed SR, MCS now begins the allocation from the SR right after the last used SR.
- **Least load-based allocation method**: Places the VMs on the least current load, determined by comparing the total number of VMs on each SR within the same machine catalog. For example, if a machine catalog contains 100 VMs distributed as follows: 20 VMs on SR1, 30 VMs on SR2, and 50 VMs on SR3, the new VMs are allocated to SR1 first. This method ensures that the load across SR1, SR2, and SR3 is balanced. You can use this method by adding a custom property Name=`"StorageBalanceType"` Value=`"VMCountBasedLeastLoad` while creating or updating a host connection.

This feature is:

- Applicable to all on-premises hypervisors (VMware, XenServer, and Hyper-V).
- Applicable to only OS disk storage.
- Not applicable to the existing VMs.

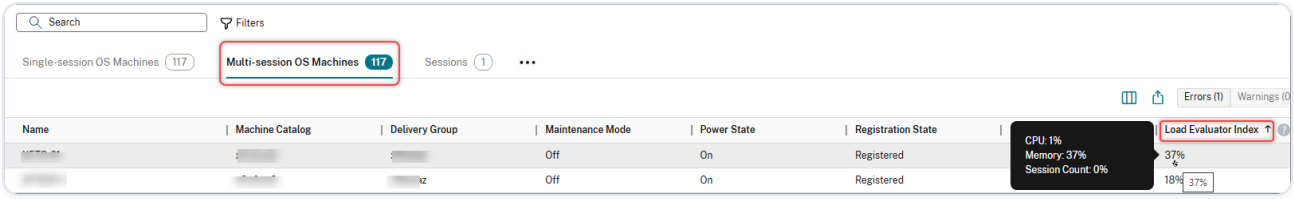
For information on creating or updating an existing host connection with the load-based allocation option, see Flexible storage location option for VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

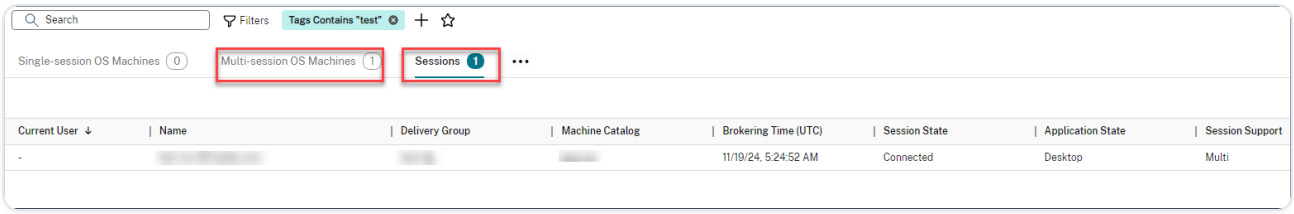
Enhanced resource monitoring for multi-session VDAs in Studio. Studio now provides detailed resource utilization and capability insights for multi-session VDAs.

Hover over the **Load Evaluator Index** column of a multi-session VDA in the **Search** node to view detailed metrics, including CPU, memory, disk usage, maximum number of sessions allowed, and more. The specific metrics displayed depend on the enabled policy settings.

This enhancement eliminates the need to run PowerShell cmdlets or navigate through multiple steps to switch to Monitor to gather this data, providing the same capabilities directly within Studio. For more information, see Machine actions.



Improved session visibility in tag-based searches. When you search for *machines* by tag in **Studio > Search**, active user *sessions* on the matching machines now appear on the **Sessions** tab. This enhancement helps prevent accidental shutdowns of machines with active sessions by providing clear visibility of those sessions, improving your management efficiency.



February 2025

New and enhanced features

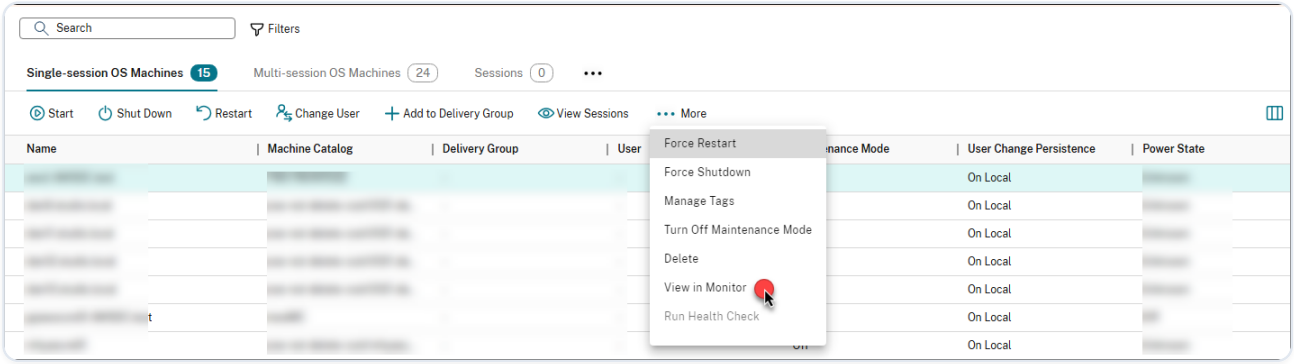
Support for provisioning data disk on Azure. You can now create and assign a persistent data disk to an MCS created persistent or non-persistent VM of an MCS machine catalog in Azure. The data disk is used for storage of persistent data like event logs, security traces, and application data.

The data disk must be provisioned from the master image. The properties such as storage type, encryption settings, zones are derived from custom properties or from the OS disk template if the properties are not specified in the custom properties. For information on creating an MCS machine catalog with a data disk, see Provision data disk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Navigate seamlessly from Studio to Monitor for machines and sessions. A new option, **View in Monitor**, is now available in **Studio > Search**, providing quicker access to detailed session and machine information in **Monitor**.

After selecting a machine or session, simply click **View in Monitor** to open its detailed view in **Monitor**. This enhancement simplifies your workflow and saves time when analyzing workload performance or troubleshooting issues. For more information, see Machine actions and Session actions.



Cost Savings by optimizing storage usage. The **Cost Savings** page now provides visibility into the amount of savings achieved through storage optimization when machines are powered Off. Previously, only compute-related cost savings were displayed. This enhancement includes the following two types of storage savings:

- **Write-back Disk**: Savings from deleting the write-back disk when a non-persistent machine is powered Off.
- **OS Disk**: Savings from downgrading the OS disk from Premium to Standard HDD when any machine is shut down.

Prerequisite:

- Autoscale must be enabled to optimize compute costs. For more information, see Get started with Autoscale.
- Change the storage type to a lower tier when a VM is shut down to optimize storage costs. For more information, see Change the storage type to a lower tier when a VM is shut down documentation.
- This feature is currently applicable only to Azure machines.

The enhancement includes:

- A report detailing storage savings from machine power-offs (autoscale or user-initiated) is now available in the **Estimated infrastructure savings** section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Total savings calculations now incorporate both compute and storage savings, broken down by source (autoscale or user action). The historical trend graph now visually distinguishes between compute and storage savings, and a tooltip provides further details on hover.
- The **Catalog details** section now includes **Compute Cost Per Hour** and **Storage Cost Per Hour**.

For more information, see Cost summary page.

NitroTPM and UEFI secure boot capability for MCS created AWS VM instances. With this feature, when creating a catalog in AWS environments, you can now select a master image (AMI) with NitroTPM and/or UEFI secure boot enabled. Accordingly, the provisioned VMs in the catalog are also enabled with NitroTPM and/or UEFI secure boot. This implementation ensures that the VMs are secured and trusted. For more information on NitroTPM and UEFI Secure Boot, see the AWS documentation. For creating a catalog enabled with NitroTPM and UEFI secure boot, see Enable NitroTPM and UEFI secure boot for VM instances.

Monitor action enhancements Citrix Monitor now provides the progress of bulk actions performed along with improvements to role based accesses on bulk actions enhancing user experience and control.

Action Progress Bar:

With this enhancement, when any action is in progress, such as a power control function (for example, restart), you can see a status of the action and a dialog box when the action is completed. This feature is applicable to all actions in the **Filters** tab. However, note that the status bar is not be available for single actions.

The progress bar shows the outcomes of bulk actions performed. Currently, customers do not know whether their action succeeded or failed and on how many sessions. This enhancement provides clarity on actions performed.

Custom role to limit bulk action option for user actions:

This enhancement allows the addition of custom roles to limit what the admin can see and control. The new custom role limits the ability to select bulk actions such as log off, disconnect, or message. This control is necessary to prevent unintentional or malicious mass actions on users.

With these enhancements, you can effectively manage and control actions within Citrix Monitor, ensuring a more secure and efficient environment. For more information, see Custom role to limit bulk action option for user actions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Option to view and troubleshoot Secure Private Access Sessions for hybrid deployments. Citrix Monitor now supports viewing and troubleshooting Secure Private Access sessions for hybrid deployments. This enhancement allows DaaS customers using Gateway, StoreFront, and Secure Private Access on-premises to monitor and troubleshoot their session data directly in the DaaS Monitor.

Previously, only cloud and on-premises deployments were visible in the Monitor. With this update, hybrid Secure Private Access sessions can now be monitored and analyzed, providing a unified view across all deployment types.

This improvement ensures better visibility, faster issue resolution, and a seamless monitoring experience for customers managing hybrid environments.For more information, see Secure Private Access integration with Monitor (Preview).

Share prepared image versions across hosting units in VMware. You can now use the **Images node** to share image versions across hosting units within the same hosting connection in VMware. This implementation ensures consistency and uniformity of images across different host units, enhancing deployment flexibility and operational efficiency. You can also use PowerShell commands to achieve this goal. For more information, see Image Management

January 2025

New and enhanced features

Support for creating MCSIO-enabled MCS machine catalogs in AWS. You can now create MCSIO-enabled MCS catalogs to create MCSIO-enabled MCS machine catalogs in AWS to improve write IOPS by directing write operations to the write-back cache and to reduce the startup time when the persisting OS disk is enabled. For more information, see Machine Creation Services (MCS) storage optimization.

Integration with Webhook Citrix Monitor now integrates with Webhook. Using this feature, you can select the required tool from the **Alerting and ITSM** section on the **Integrations and data exports** page and then click **Get Started**. This gives you reference links to create the tool specific channel and webhook URL, which is the first step. Once the first step is completed, you can create webhook profiles.

You can also create webhook profiles in the **Integrations and data exports** > **Developer tools** page of Citrix Monitor. You can find steps and resources to integrate the following alerting and ITSM tools with Citrix Monitor:

- Slack

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microsoft Teams
- ServiceNow

This feature helps you to send alert notifications to the preceding third-party applications that have incoming webhook URLs configured.

Key features:

- New integration tiles for Slack, Teams, ServiceNow, and other supported platforms
- Navigation to the FTU page for each integration
- Create or edit webhook configuration page with a UI workflow to provide webhook URL, headers, body, and test the webhook configuration and save it
- List the webhook profiles created and provide the capability to edit or delete the webhook profiles
- Map created webhook profiles with the advanced alert policies

For more information, see Integrations and data exports page.

Add applications to existing AWS deployments in Quick deploy node. You can now add applications to existing AWS deployments thus simplifying the overall deployment process. For more information, see Create a deployment.

Option to reset In-Use Active Directory (AD) accounts. With Studio you can now reset machine Active Directory (AD) accounts even when the status of the machine is In Use. This is necessary because sometimes the system does not correctly detect when a machine is in a tainted state.

Alerting admins that power policies remain effective when disabling Autoscale. The enhancement is to remind the admins that disabling Autoscale does not affect the power policy settings for a delivery group. This ensures that admins are aware of the scope of Autoscale disabling and clarifies that power policies remain effective when Autoscale is turned off.

Filter master images based on hosting unit regions. During machine catalog creation for the Azure platform, Studio can now filter out and exclude master images that belong to different regions other than the hosting unit's region. This ensures that only images from the same region as the hosting unit are available for selection. For more information, see Create a machine catalog from the Machine Catalogs node.

MCSIO with only disk cache is no longer supported. The option to configure MCSIO with only disk cache (without memory cache) has been removed across all hypervisor and cloud service environments. When creating machine catalogs with the MCSIO enabled, you must now set a non-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

zero memory cache size. In addition, you can't edit catalogs configured with only a disk cache until you set a memory cache size. For more information, see Configure cache for temporary data.

Creating AWS VMs using machine template properties is no longer supported. Support for creating AWS VMs by capturing machine template properties has been removed as part of the transition to creating VMs using machine profiles. The **Apply machine template properties to virtual machines** option has been removed from the **Machine Template** page. Instead, you can create AWS VMs using machine profiles for a similar and more streamlined experience. For more information, see Create a machine profile-based machine catalog using Studio and Create a machine profile-based machine catalog using PowerShell.

Support for creating MCSIO enabled MCS machine catalog in AWS. In the AWS environment, you can now create MCS Storage Optimization (MCSIO) enabled non-persistent catalog using PowerShell commands. To create such a catalog, you must install the MCSIO driver while installing or upgrading the VDA. By default, that driver is not installed. For more information on creating the MCSIO enabled catalog, see MCSIO enabled catalog. The option to configure MCSIO with only disk cache (without memory cache) using Studio has been removed across all hypervisors and cloud service environments.

Least used and unused published apps report. The **Applications** page now offers detailed usage information for published apps accessed through the Citrix Workspace app, empowering administrators to optimize app management and resource allocation.

This feature helps in understanding the application usage patterns within the organization and enables customers to make data-driven decisions to help make their Citrix deployments more efficient.

NOTE:

This feature is available only for the platinum-licensed sites.

The enhanced **Applications** page includes a usage section that shows the following:

- **Total published apps:** Identifies the total number of published apps.
- **Least used apps:** Helps to make informed decisions about retaining or removing rarely used apps, optimizing resource allocation, and license management. This section lists the following:
  - **Distinct users in the last 30 days**
  - **Total launches**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

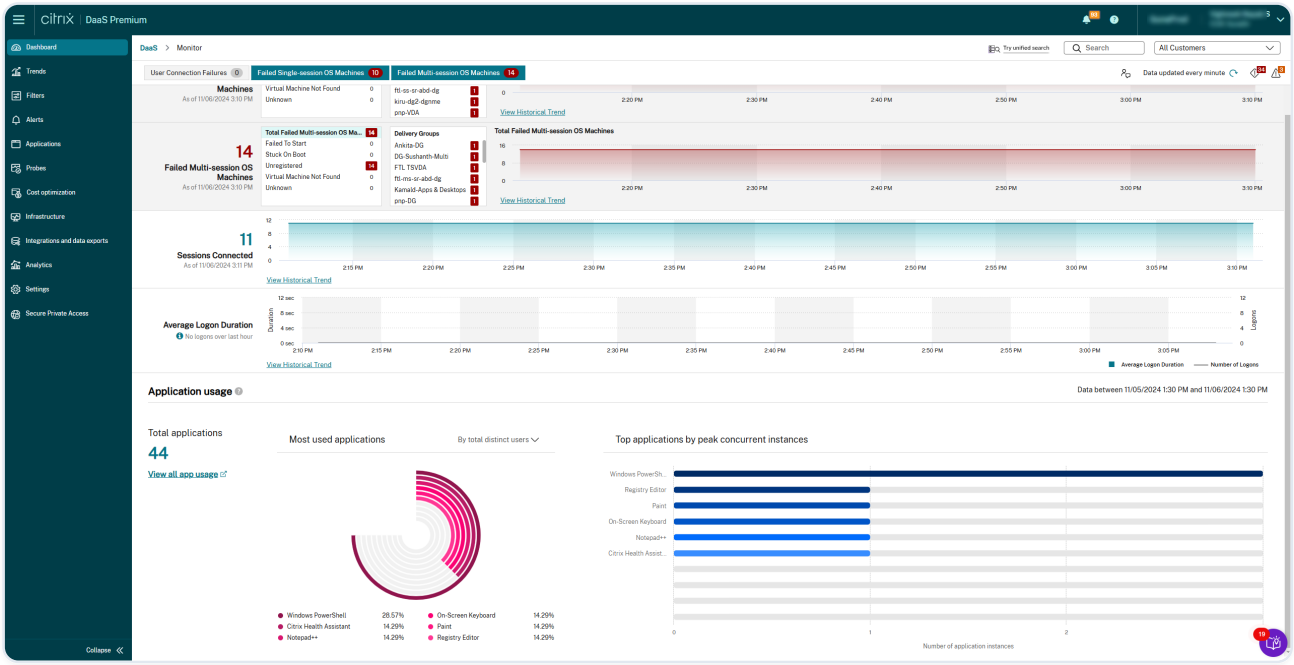
- **Peak concurrent instances**
- **Trend chart:** View a graph showing distinct users over time.

- **Not used apps:** Helps to identify unused apps to free up memory, configuration resources, and potentially save on licensing costs. This section lists the name of the apps, the corresponding delivery group, and the state of the app.

You can also use the **Export** option to export the data in the **Least used** and **Not used** sections.

NOTE:

Currently, only published apps (desktop apps in Citrix Workspace app) are included in this enhancement.



For more information, see the Least used and unused published apps report documentation.

Secure Private Access integration with Monitor (Preview). The Secure Private Access integration with Monitor allows admin to monitor and troubleshoot all Secure Private Access sessions in Monitor.

Available actions include viewing the details of the following:

- Secure Private Access active sessions for a user under the Select a Session popup > Active Sessions tab
- Secure Private Access failed or blocked enumerations and failed app launches under the Select a Session popup > Denied Access tab

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Session and application details view for active and failed app launches, as well as for failed and blocked enumerations

For more information, see Secure Private Access integration with Monitor (Preview) page.

December 2024

New and enhanced features

Automated configuration tool commands for backup and restore. With this feature, you can use PowerShell commands supported by Automated configuration tool to trigger the backup and restore APIs that Studio uses. For more information, see Automated configuration tool cmdlets for backup and restore.

New permission for orphaned resource detection in Citrix DaaS. Previously, only **Full Administrator** or **Cloud Administrator** roles could perform orphaned resource detection. With the introduction of a **Use Host Connection to Detect Orphaned Resources in Hypervisor** permission to the **Hosts** category, any roles assigned with this permission can now detect orphaned resources. For more information, see Detect Orphaned Azure resources and Retrieve a list of orphaned resources.

Get started with Citrix DaaS on Google Cloud. Integrating Google Cloud Platform (GCP) with Citrix DaaS and deploying the first set of virtual desktops involves a series of sequential steps, making it a relatively intricate process. To simplify this process for administrators, a streamlined deployment experience, similar to AWS WorkSpaces Core's Quick Deploy feature, has been introduced. This streamlined onboarding process aims to increase GCP adoption, prompting Google's sales teams to collaborate with Citrix in customer engagements. Also, it opens avenues for Citrix sales teams to engage with customers who prioritize Google-centric solutions. For more information, see Quick Deploy for Google Cloud.

Full Configuration: Support for selecting launch template as machine profile for AWS. When provisioning AWS VMs using MCS, you can now select a launch template as the machine profile. For more information, see Select an image and a machine profile.

Multi-select policies. You can now select multiple policies and checkout the following enhancements:

- Click a policy row: If you click a policy row, the actions bar at the top shows actions of a single policy. The details pane at the bottom provides information about the policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Select the check boxes of multiple policies: If you select the check boxes of multiple policies whose statuses are either enabled or disabled, then the actions bar at the top shows actions of multiple policies. The details pane at the bottom displays the number of policies selected.

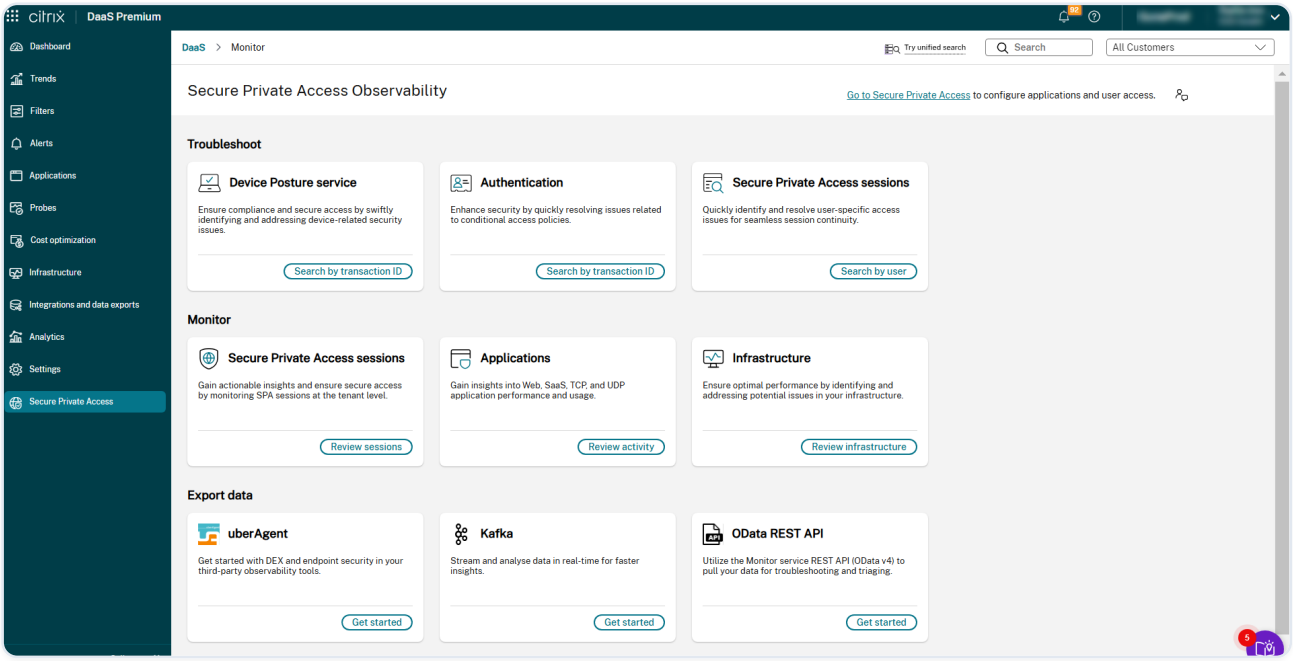
NOTE:

After you select multiple policies, you can view the details of another single policy by clicking the row of that policy. This action does not clear the previously selected policies. However, the right-click action does not display the actions for that policy row.

GCP catalogs support inheriting the machine type settings from machine profiles. When creating MCS-provisioned machine catalogs in GCP environments, the machine type now defaults to the size specified in the selected machine profile. If necessary, you can manually adjust this setting. For more information, see Create a machine catalog using Full Configuration interface.

Clarity on dependent policies. Some settings are dependent on other settings. For example, a child setting might be configured, but if its parent setting is not enabled, the child setting configured does not take effect. The dependencies were not clear before. Starting with this release, clarity is provided on which are the parent policies that must be configured first before you can configure the child policies. For more information, see Policy settings.

Secure Private Access tab on Monitor. The **Secure Private Access** tab on Monitor provides a dedicated place for all new features related to Secure Private Access. This tab offers details on the supported functions for Secure Private Access, giving administrators a central location to access and manage these features.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Key benefits:

- Centralized information: Administrators can easily see all supported troubleshooting features for Secure Private Access in one place.
- Enhanced observability: The new left navigation bar in the Monitor UI lists all Secure Private Access services, including Secure Private Access sessions, applications, and device posture, providing better observability.
- Improved navigation: The Secure Private Access tab includes hyperlinks to different pages, making it easier for administrators to navigate to various features and functions.

For more information, see Secure Private Access tab on Monitor.

Visibility for Secure Private Access Service. To provide detailed monitoring and visibility for Secure Private Access applications and users, Monitor is now enhanced to include Secure Private Access session visibility. The **Filters** tab and **Dashboard** provide detailed Secure Private Access session information.

Key features:

- **Filter Secure Private Access Sessions**: You can now filter Secure Private Access sessions in the **Filters** > **Sessions (Web, SaaS, and TCP/UDP)** tab.
- **Filter Secure Private Access Applications**: You can also filter Secure Private Access applications in the **Filters** > **Applications (Web, SaaS, and TCP/UDP)** tab.
- **App Failures and Active Sessions**: Monitor app failures for web/SaaS and TCP/UDP apps, and view active sessions for web/SaaS apps in the Dashboard.

For more information, see Visibility for Secure Private Access Service.

Unified platform experience for Citrix Monitor. Citrix Monitor is now aligned with all other components within Citrix Cloud, providing a unified platform experience. The user interface has been refreshed with a modern look and feel, offering easier navigation and better data representation. The enhanced interface is intuitive and designed to help users easily comprehend the data needed to monitor and troubleshoot Citrix sessions.

Enhancement to Connections tab. The **Connections** tab now offers streamlined navigation for quicker troubleshooting. From the **Filters** tab > **Connections** page, you can directly access:

- **Activity Manager**: Click the **Associated User** or **Endpoint name** to view the respective Activity Manager details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Machine Details page**: Click **Machine Names** to see comprehensive machine information, including machine details, utilization details, infrastructure details, and applied hotfixes. For more information, see Troubleshoot Machines. This enhancement simplifies navigation, enabling faster resolution of connection-related issues.

For more information, see Filter data to troubleshoot failures.

Filter resource location details. You can now view the resource location for single-session or multi-session OS machines in the **Filters** > **Machines** tab. This enhancement allows you to quickly identify and address issues related to specific resource locations, leading to a smoother user experience.

To display the new **Resource Location** column, go to **Choose Columns** and select **Resource Location** in the **Filters** > **Machines** tab.

Enhancement to Session Performance tab. The **Session Topology** section of the **Session Performance** tab is enhanced to include the following endpoint metrics which exist in the Citrix Workspace app for Windows, Mac, Linux, HTML5, or Chrome:

- Public IP address
- Internet Service Provider
- Location such as country or city
- Whether the Citrix Workspace app session is opened in native app or browser (HTML5)
- Accessed using Workspace or StoreFront
- Resource utilization such as CPU %, Memory %, and GPU (Overall %)
- Network latency

This enhancement helps to troubleshoot issues regarding sessions quickly. For more information, see Session Performance metrics.

Machine net active usage. The **Workload rightsizing** page now includes detailed insights into machine net active usage, providing the following details:

- Percentage of net active usage
- Average machine uptime
- No session time
- Idle time
- Disconnected time

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature allows you to see detailed machine usage information, enabling you to optimize costs accordingly.

For more information, see Workload rightsizing.

Cloud Connector health monitoring. The Cloud Connector component is now added to the **Infrastructure Monitoring** dashboard. Cloud Connectors are automatically onboarded when a connection between Citrix Cloud and your resource locations is established.

This feature enables administrators to monitor the health of Cloud Connectors using a single dashboard view and proactively configure alerts.

NOTE

.

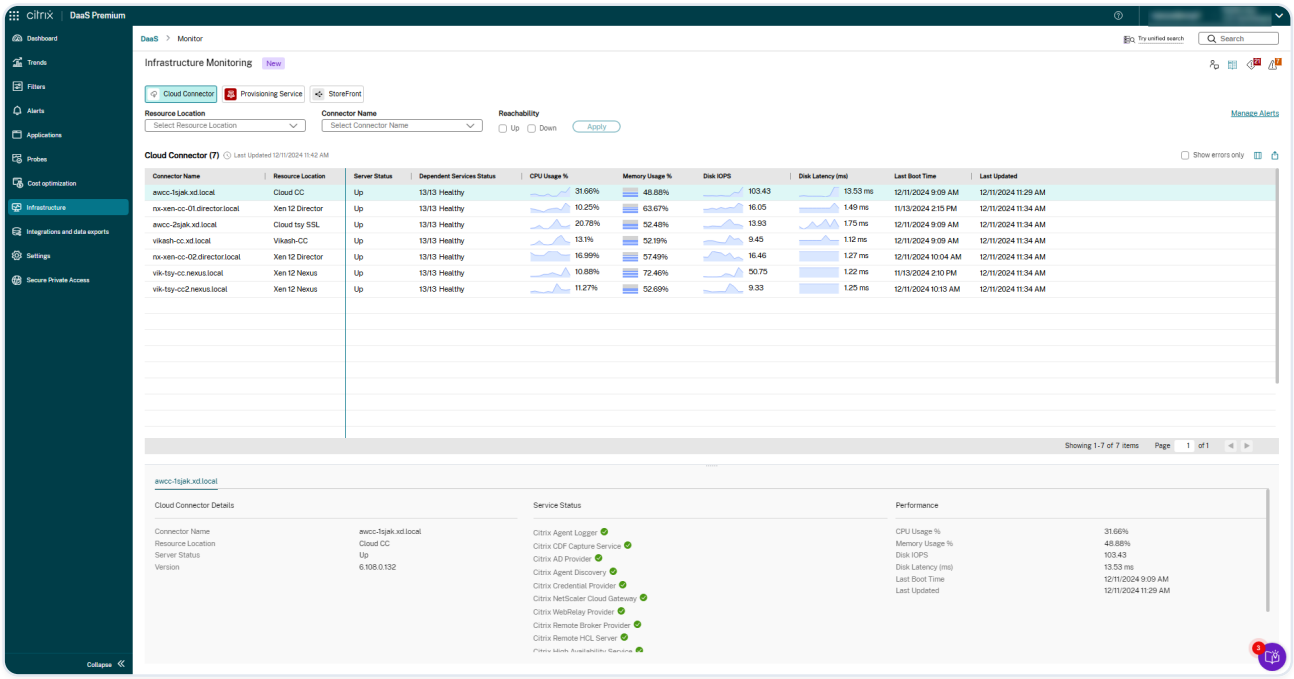
The `citrixinframonitor.msi` is not required to be installed for monitoring Cloud Connectors.

Benefits:

- **Comprehensive monitoring**: Visibility into critical health indicators for the Cloud Connector such as high availability, connection lease exchange, and AD provider, and so on
- **Configurable alerts**: You can configure alerts on health metrics of interest, define severity, and scopes for admins to receive detailed alerts according to the alert configuration.

To monitor the Cloud Connector, click the **Infrastructure** tab on Monitor. The **Infrastructure Monitoring** page opens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can also view the details of all the services status in the **Cloud Connector Details** section.For more information, see Cloud Connector health metrics.

Support for creating Citrix Provisioning catalogs in VMware environments using Studio. With Studio, you can now create Citrix Provisioning catalogs in VMware environments. Previously, you had to switch between different consoles to provision and manage those catalogs. This feature simplifies the process, letting you perform provisioning and power management tasks entirely within Studio. For more information see, Create a Citrix Provisioning catalog in VMware environment using Studio.

Delivery of app attach disks as CimFS. Previously, only delivery of app attach disks as virtual disks (VHD and VHDX) was supported. With this feature, delivery of app attach disks as Composite Image File System (CimFS) is also supported. For information, see Store application packages on network shares.

Optimize storage load balancing with the least load method. Previously, Machine Creation Services™ (MCS) used a round-robin method to distribute VMs across storage repositories, often leading to uneven storage utilization.

Studio now introduces the **Optimize storage load balancing with least load method** option. If you select two or more OS data storage locations during catalog creation, this option becomes available, enabling disks to be allocated to the least loaded storage repository.

This feature enhances load balancing and improves system stability, and it's supported in XenServer, VMware, and SCVMM virtualization environments. For more information, see Step 3. Storage selection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Autoscale powers on hibernated VMs. With this feature, in Azure, autoscale can power on hibernated multi-session Remote Desktop Services (RDS) and shared single session VMs with no sessions on it during peak time. The VMs can be of MCS and non-MCS machine catalogs.

Support for NVMe-only SKUs in Azure. Previously, MCS supported only SCSI storage controller type. With this feature, MCS also supports the NVMe storage controller type to support the new VM SKUs on Azure. For information on NVMe, see the Microsoft documentation General FAQ for NVMe. For information on creating an MCS machine catalog using a service offering that:

- supports both SCSI and NVMe, see Create a catalog using a service offering that supports both SCSI and NVMe
- supports only NVMe, see Create a catalog using a service offering that supports only NVMe

Set a default time zone for your Citrix DaaS site. With Studio, you can now set a default time zone for your Citrix DaaS site. To complete this task, go to **Settings > Date and Time**. Studio uses this time zone for all time displays and scheduling such as scheduled restart and autoscaling. This setting makes it easier to manage time and ensure time consistency across your site. For more information, see Time zone setup.

If needed, you can change the time zone for individual resources. For example, you can set a different time zone for a delivery group that serves machines in a different region. For more information, see Change user settings in a delivery group.

Studio aligns with Citrix Cloud's unified navigation experience. As part of the shift towards a unified navigation experience across the Citrix Cloud platform, we've updated Studio to align with this platform-wide initiative. Key changes include a green background for the navigation pane and breadcrumb navigation for easier access. These updates enhance usability and drive feature adoption, making it easier to discover and manage resources. For more information, see Studio.

Support for AWS on-demand provisioning. Previously, when you would shut down a non-persistent VM in AWS, the OS disk did not get deleted. Now, with on-demand provisioning, the OS disk gets deleted when you shut down a non-persistent VM. This implementation of AWS on-demand provisioning saves cost when the VM is not in use. For more information, see AWS on-demand provisioning.

Show Secure Default Settings. This feature shows the secure default setting along with the default setting for a policy. The default setting might be overwritten by the secure default setting. If the secure default setting is enabled, during VDA installation, the priority of the policy settings is affected as follows:

- Customized setting takes the highest priority

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Secure default setting takes the second priority
- Default setting takes the least priority

For more information, see Policy settings.

Displaying policy details in Device Posture Events. You can now view Device Posture policy evaluation details as part of Device Posture events on Citrix DaaS Monitor. The different states of the policy evaluation and error codes are displayed. This feature simplifies the triage and troubleshooting of user issues. For more information, see the Diagnose Device Posture events failure page.

November 2024

New and enhanced features

Image management is now Generally Available. Image management functionality is now generally available for Azure and VMware virtualization environments. Also, the **Images** node now allows you to share image versions across hosting units within the same hosting connection in Azure. This implementation ensures consistency and uniformity of images across different host units, enhancing deployment flexibility and operational efficiency. You can also use PowerShell commands to achieve this goal. For more information, see Image Management.

WebSocket communication. With this feature, you can set up a WebSocket connection for communication between VDAs and Delivery controllers as an alternative to using WCF communication. For more information, see WebSocket communication between VDA and Delivery Controller.

Studio support for a snapshot of the disk or an OS image of the disk as a master image in the GCP. In the GCP virtualization environment, you can now select a snapshot of the disk or an image of the disk as a master image while using Studio to create an MCS machine catalog. The snapshot of the disk or an image of the disk can be regional and multi-regional as compared to the VM instance which is only regional. This feature significantly simplifies image management workflow and reduces the time and effort required for image management in GCP. For information on creating an MCS catalog in GCP using Studio, see Create a machine catalog.

Connecting Citrix Components from the UI. Admins can use the Monitor UI to register their Citrix components for Infrastructure Monitoring. After installing `Citrixinframonitor.msi`, the UI-based workflow can be used to complete the registration process without needing to use PowerShell commands. This enhancement simplifies the process of registering, deregistering, and updating Citrix components.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The new **Connect Citrix components** page allows you to manage connections between Citrix components and the Citrix DaaS site. You can also view the available connections from Provisioning Service and StoreFront on this page.

These updates streamline the management and integration of Citrix components, making it easier to maintain and monitor your infrastructure.

For more information, see Step 2: Register Citrix Infrastructure Monitor on Monitor UI.

Enhancement to Advanced Alert Policies. Alerts related to Infrastructure Monitoring, previously known as Infrastructure policies, are now part of Advanced alert policies.

You can select the dependent services based on the selected data source and create alerts for Cloud Connectors as well.

NOTE:

The existing Infrastructure policies created for Provisioning Service and StoreFront are migrated to the Advanced alert policies section.

For more information, see Advanced alert policies.

Support to configure secondary VMs scale up or scale down list for MCS-created catalogs on Azure. Web Studio now enables the administrators to define secondary VMs to scale up and scale down the MCS-created catalogs on Azure. Based on the usage of CPU and memory resources, if the CPU or memory usage exceeds a certain threshold, the system will automatically use the secondary VMs to handle the load. Alternatively, if the usage falls below a certain level, the system will automatically shut down some VMs to conserve resources. For more information, see Create a machine catalog using an Azure Resource Manager image in Studio.

Delivery group details enhanced with policy information. We've enhanced the **Details** view for Delivery Groups by adding a dedicated tab that shows policies assigned to the selected group. This improvement simplifies policy management, configuration, and troubleshooting for delivery groups by providing quick access to relevant policy information.

Support for multi-region snapshot of the disk or an image of the disk as master image in GCP. A snapshot or an image of a disk in GCP can be regional or multi-regional. Regional snapshots and disk images are tied to a particular region, example, `us-central1`, whereas multi-regional snapshots and disk images are tied to a geo-location, example, `US`. With this feature, you can use a multi-region snapshot of the OS disk or an image of the disk as master

© 1997–2026 Citrix Systems, Inc. All rights reserved.

image input when creating MCS machine catalogs in GCP. You can see the list of all snapshots (both regional and multi-regional) under `snapshots.folder` location and disk images (both regional and multi-regional) under `images.folder` under hosting unit inventory path.

Support for converting a non-machine profile-based machine catalog to machine profile-based machine catalog in VMware environment. In the VMware environment, you can now use a VMware template as a machine profile input to convert a non-machine profile-based machine catalog to a machine profile-based machine catalog. New VMs added to the catalog take property values from the machine profile. For more information, see Convert a non-machine profile-based machine catalog to machine profile-based machine catalog.

Support for Windows Server 2025. Citrix Virtual Apps and Desktops now supports Windows Server 2025. For more information on Windows Server 2025, see the Microsoft documentation What's new in Windows Server 2025.

Studio: Support for provisioning persistent VMs on Windows Server OS using Full Copy Clone. Studio now supports provisioning persistent VMs on Windows Server OS using the Full Copy Clone approach. This approach improves data recovery and migration capabilities and can help reduce IOPS after machines are created. For more information, see Select a desktop experience and Virtual machine copy mode.

Studio AWS Quick Deploy: Support for adding non-BYOL-enabled AWS accounts. Studio now allows you to connect an AWS account without enabling BYOL feature for a region. You can configure the BYOL feature for a region later. The account without BYOL enabled for a region has a restriction of selecting only default tenancy images and shared directory connection to continue to setup the account. For more information, see Connect your AWS account.

Backup and restore using Studio is now Generally Available. You can now use the Backup and Restore node available in the left pane of your Manage DaaS console. This feature enables you to create on-demand and scheduled backups and restore deleted applications, policies, and more. For more information, see Backup and Restore using Studio.

Configuration guides widget on the Studio Home Page. We've updated the Studio **Home** page by renaming the **Get started** widget to **Configuration guides**. This widget now includes the original **Get Started with DaaS** guide and a new **Check resiliency configurations** guide.

Check resiliency configurations guide. We've introduced a new **Check resiliency configurations** guide in the **Configuration guides** widget on the Studio **Home** page. This guide provides checklists for verifying resiliency settings across various types of StoreFront deployments:

- Checklist for on-premises StoreFront deployments

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Checklist for Citrix® StoreFront Cloud deployments
- Checklist for mixed StoreFront deployments

Following this guide, you can verify Local Host Cache and Service Continuity are properly configured in your deployment, ensuring uninterrupted access to apps and desktops during service disruptions.

DaaS get-started guide now generally available. The **Get-started with DaaS guide** streamlines and simplifies the DaaS deployment process for both new and experienced administrators. This guide walks you through setting up your DaaS deployment by asking a series of questions to guide the configuration. For more information, see Use DaaS get-started guide.

Enhanced domain selection. A new option in the UI now allows you to enter a domain name for an exact match wherever domain selection is needed. This enhancement offers these benefits:

- Faster searches: You can skip browsing large directories, getting results directly and instantly.
- Time savings: Eliminates full-directory loading, speeding up workflows.
- Enhanced experience: Improves admin management efficiency, especially in environments with large directories.

Validate configuration before creating an MCS machine catalog in AWS environments. With this feature, you can now validate configuration settings before creating an MCS machine catalog in AWS environments using the parameter `-validate` in `New-ProvScheme` command. After you run this PowerShell command with the parameter, you get an appropriate error message if there's an incorrect parameter used or a parameter has conflict with another parameter. You can then use the error message to resolve the issue and successfully create an MCS machine catalog using PowerShell. This feature is applicable to AWS, Azure, GCP, and VMware virtualization environments. For more information, see Validate configuration before creating an MCS machine catalog.

Update to Performance Metrics panel. The **Performance Metrics** panel has an enhanced visualization of the historical data metrics. When you click the **Session Performance** tab, along with the last 15-minutes data, you can view the last 48 hours data for ICARTT and ICA® Latency. This enhancement helps to reduce mean time for resolution by enabling admins to triage issues even though the session was terminated in the last 48 hours.

For more information, see the Performance metrics section.

Enhancement to Filters tab. With this release, the following extra filters are added to the **Sessions** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **All** - Displays all sessions
- **Active, Connected, and Disconnected** - Displays only the active, connected, and disconnected sessions.
- **Ended** - Displays only the sessions that have ended within the last 48 hours. The default filter is **Active, Connected, and Disconnected**.

Enhancement to ended session . In the ended session (formerly historical session), the **Session Performance** tab shows data for the last 48 hours. Also, you can view the **Session Logon** tab for the ended session.

For more information, see the Diagnose ended user sessions [Preview] page.

October 2024

New and enhanced features

Policy sets now generally available. Policy sets are collections of rules and guidelines that allow simplified, role-based, and easy management operations. Policy sets allow you to create logical divisions within your administrator team, organizations, or machines. You can assign scopes and delivery groups so that authorized administrators can manage the relevant policies for users and machines. For more information, see Policy sets.

Enroll persistent machines of hybrid Azure AD joined type into Microsoft Intune for co-management. During machine catalog creation, you can now enroll persistent machines of the hybrid Azure AD joined type into Microsoft Intune (with Configuration Manager) for co-management. This feature applies to single and multi-session, persistent VMs and on all hypervisors and cloud services, ensuring uniform device management across your infrastructure. This feature is applicable only to VDA version 2407 and later.

For more information, see Hybrid Azure AD joined catalogs enrolled in Microsoft Intune and Create Hybrid Azure AD joined catalogs enrolled in Microsoft Intune.

Diagnose conditional authentication failures. Whenever any conditional authentication fails, you can use the transaction ID available in the failure message and search in the Monitor for the failure details. Monitor helps you to troubleshoot conditional authentication failure events by displaying failure reasons and conditional policies on the Monitor UI. For more information, see Diagnose conditional authentication failures.

Service accounts for machine identity management. MCS has developed a new mechanism for managing on-premises Active Directory and Azure Active Directory (Azure AD) identity service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

accounts to simplify and enhance the management of machine identities including computer accounts in on-premises Active Directory, Azure AD joined devices and Intune enrolled devices. Firstly, we have introduced on-premises Active Directory service account support which allows administrators to manage computer accounts in on-premises Active Directory without having to enter domain credentials every time. Secondly, we have introduced Azure AD identity Service Principal Names (SPN) support which allows administrators to manage Azure AD joined or Intune enrolled devices in the Azure AD tenant, in a secure and streamlined manner. Lastly, we have implemented a new mechanism for service account management in our Studio, simplifying the process and making it easier to maintain security and compliance. For more information, see Service accounts for machine identity management.

Support to select an Instance template as a machine profile. When creating MCS machine catalogs in GCP environments using Studio, you can now select Instance Templates as the inputs for machine profiles. Also, the Customer-Managed Encryption Key (CMEK) settings follow a priority sequence. For more information, see Create a machine catalog using Studio

Export a machine profile to an ARM template spec. Studio now supports exporting the machine profile used by a catalog into an ARM template spec. With this feature you can easily reuse an existing machine profile as a template and modify it for future provisioning needs. For more details, see Export a machine profile as an ARM template spec.

MCS catalogs: AWS launch templates support. You can now use AWS launch templates as machine profiles when creating or editing MCS catalogs in your AWS environment. AWS launch templates are available in the machine profile list for selection.

Retrieve Connector Appliance information. With this feature, you can use the PowerShell command `Get-ConfigEdgeServer` to retrieve the Connector Appliance information.

- `Get-ConfigEdgeServer -ConnectorType 'Unified'`: Returns Connector Appliance information
- `Get-ConfigEdgeServer -ConnectorType 'Windows'`: Returns only edge servers information
- `Get-ConfigEdgeServer`: Returns only edge servers information.

Reboot schedules for hibernated VMs. With this feature, you can configure reboot schedules for hibernated VMs if the Delivery Group is hibernation enabled. In the reboot cycle, the VMs are resumed and, then shut down. The reboot schedule can be set as weekly, daily, monthly, and once. You can configure multiple schedules. Note that VMs resuming from hibernation can take few mins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data caching for the Images node. We've introduced data caching for the **Images** node to improve the overall user experience. This enhancement significantly reduces the page load time when you navigate to the **Image definition** and **Image versions** lists, as well as the **Details** and **Image Scheme** tabs.

Configuration logs labeling. You can now label configuration logs on the **Logs > Events** tab, facilitating the identifying and exporting of logs. In addition, the **Logging** node now offers enhanced features, including exporting logs to CSV files, advanced search, and table-style display for the **Events** tab. For more information, see View configuration log content.

Support for creating a host connection using Azure Managed Identity. Previously, you could create an Azure hosting connection using a service principal. This required providing and storing of the application ID and secret of the service principal. The Azure Managed Identities offers a secure and scalable way to access Azure services without the need to manage credentials. This approach eliminates the risks associated with storing, rotating, and managing secrets. Managed identities also support automatic token refresh, ensuring that applications always use valid credentials without any additional code for token lifecycle management.

With this feature, you can create a host connection to Microsoft Azure Resource Manager using Azure Managed Identity. Currently, you can create the host connection using only PowerShell commands. For information on creating a host connection using Azure Managed Identity, see Create a host connection using Azure Managed Identity.

Support for Boot Integrity Monitoring in Azure. With this feature, in Azure virtualization environments, you can enable Boot Integrity Monitoring for MCS machine catalog VMs (persistent and non-persistent VMs) using a machine profile (VM or template spec) that has GuestAttenstation extension installed. Boot Integrity Monitoring is only supported for Trusted Launch and Confidential VMs that use Secure Boot and virtual Trusted Platform Module(vTPM).

If your VM has Secure Boot and vTPM enabled, and GuestAttestation extension installed, Microsoft Defender for Cloud can remotely validate that your VM boots correctly. This monitoring is called Boot Integrity Monitoring. For more information on boot integrity monitoring, see Boot integrity monitoring overview.

For information on creating a catalog enabled with boot integrity monitoring, see Boot Integrity Monitoring.

Filter empty resource groups. With this feature, you can filter out empty resource groups while selecting a master image, machine profile, or prepared image during the machine catalog creation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can do this using a PowerShell command `Get-HypInventoryItem`. For more information, see Filter empty resource groups.

Support for creating preformatted WBC disk catalogs in Azure. With this feature, in Azure virtualization environments, you are able to utilize a preformatted WBC disk for newly created catalogs. This action significantly reduces the time required to start each VM of an MCS or MCS provisioned Citrix Provisioning™ machine catalog. To implement this functionality, create an Azure catalog with WBC enabled and include an additional custom property `PreformatWriteBackCache` as `True`.

You can update an existing catalog using the `Set-ProvScheme` command to update the WBC disk size.

This feature is compatible with the Image management workflow where MCS separates the mastering phase from the overall provisioning workflow. For more information, see Create a preformatted WBC disk catalog.

Delete WBC disk at shutdown for MCS provisioned Citrix Provisioning catalogs. With this feature, you have the option to delete the write-back cache (WBC) disk after you shut down the VM for MCS provisioned Citrix Provisioning catalogs in Azure. This implementation helps to save cost when you do not need a persistent WBC disk. This feature is also applicable to an existing catalog. For more information, see Delete WBC disk at shutdown for MCS provisioned Citrix Provisioning catalogs.

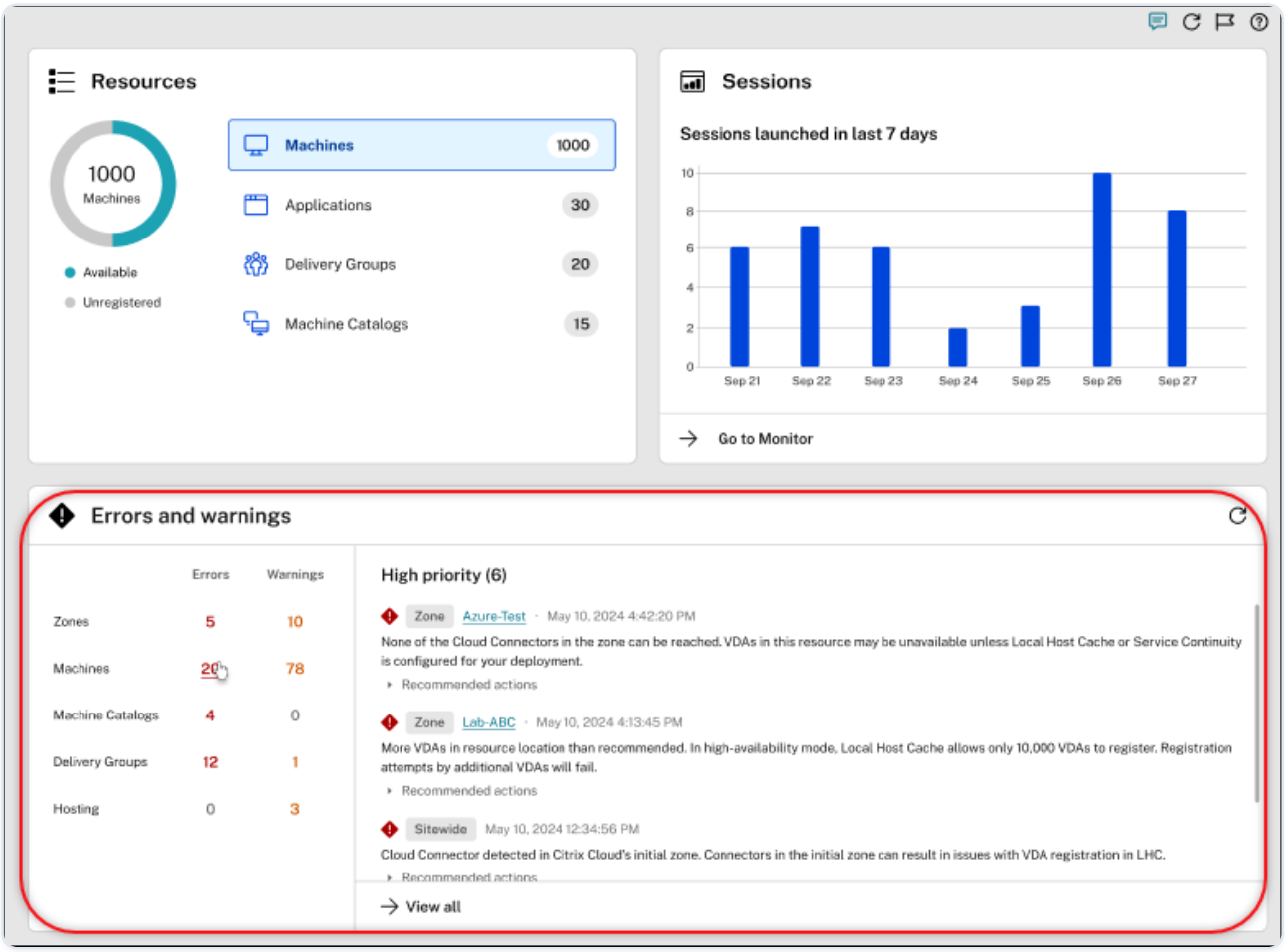
Support for creating a network security group. With this feature, you can now create a Deny-All network security group for image preparation instead of requesting Citrix to create and modify a network security group automatically. Edit the custom properties of the hosting unit using a PowerShell command `Set-Item` to include the parameter `NsgForPreparation` to provide the Deny-All network security group. For more information on using the PowerShell command, see Use a pre-created network security group.

Support for using Azure temporary disk as a WBC disk for existing MCS machine catalogs. With this feature, you can now use Azure Temporary disk as a write-back cache (WBC) disk for existing MCS machine catalogs and existing VMs. Use the `Set-ProvScheme` PowerShell command to update existing catalogs. This implementation saves storage cost because Azure temporary disk is free of charge. For information on the steps, see Use temporary disk as WBC disk for existing catalogs.

Errors and warnings center. With a new widget, **Errors and warnings**, on the Studio **Home** page, you can now view all errors and warnings from your DaaS deployments in one place. This

© 1997–2026 Citrix Systems, Inc. All rights reserved.

widget streamlines issue resolution by consolidating scattered alerts, enhancing visibility, and reducing troubleshooting time. For more information, see Home page.



Enhancement to Trends page. The **Trends** page now features two new banners linking to the **Cost optimization** page, providing quicker access to cost-saving information and reports. The **Machine Usage** tab now includes links to **Estimated Savings** and **Savings report**, while the **Resource Utilization** tab offers a link to **Workload rightsizing** (formerly known as **Infrastructure rightsizing**). These enhancements streamline navigation and improve visibility, enabling users to make data-driven decisions for cost optimization. For more information, see the Trends page.

September 2024

New and enhanced features

Backup and restore using Studio (Preview). You can now use the **Backup and Restore** node available in the left pane of your Manage DaaS console. This feature enables you to create on-demand and scheduled backups and restore deleted applications, policies, and more. For more information, see Backup and Restore using Studio (Preview).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Validate permissions on host connection in Azure. Previously, in Azure environments, you could validate only the host connection credentials (client id or application id) used to create a connection to Azure.

With this feature, you can:

- Get the list of permissions assigned to your host connection credential
- Get the list of operations that can be performed with the permissions assigned
- Information on the permissions required
- Information on how to add the desired permissions

This helps you to troubleshoot and get necessary permissions ahead of time so that you can perform the tasks without being blocked. For more information, see Validate permissions on host connection.

Create Citrix Provisioning catalogs using MCS PowerShell commands in XenServer. You can now create Citrix Provisioning catalogs using MCS PowerShell commands in XenServer environments. You can create both machine-profile based and non-machine profile based Citrix Provisioning catalogs. For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

Repair the identity information of active computer accounts in GCP, SCVMM, and XenServer. In GCP, SCVMM, and XenServer environments, you can now reset the identity information of active computer accounts that have identity-related problems. You can choose to reset only the machine password and trust keys, or reset all configuration of the identity disk. This implementation is applicable to both persistent and non-persistent MCS machine catalogs. Currently, the feature is supported for AWS, Azure, GCP, SCVMM, VMware, and XenServer virtualization environments. For more information, see Repair the identity information of active computer accounts.

Support for creating Azure AD joined catalogs enrolled in Microsoft Intune for non-persistent VMs. You can now create Azure AD joined catalogs enrolled in Microsoft Intune for non-persistent single-session and multi-session. This feature is applicable only to VDA version 2407 and later.

For information on requirements, limitations, and considerations on Microsoft Intune enabled catalogs using Citrix DaaS, see Microsoft Intune.

For information on creating Microsoft Intune enabled catalogs, see Identity pool of Microsoft Intune enabled machine identity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

New application publishing option for associating file types with applications. We've added an option, **File Type Association**, for publishing applications in Studio. This feature enables you to specify and manage extensions for applications when publishing them:

- When you add Local App Access applications, this option appears in the left pane.
- When you add an application for delivery or application groups, this option is accessible through the **Properties** menu of the application.

This enhancement ensures a more comprehensive and streamlined application publishing experience.

Enhancements to the Preview widget. We've enhanced the **Preview** widget in Citrix DaaS, providing a more streamlined and user-friendly preview experience. The enhancements include:

- **Preview activity logging.** Enabling or disabling preview features are now recorded in the Logging node. This feature ensures visibility into the activation and deactivation of preview features for audit and troubleshooting purposes.
- **Contextual information.** Supplementary content for preview features is now available to improve your understanding of each preview feature. The information includes links to installation packages, demo videos, Podio forms, preview articles, blogs, and other relevant documentation.
- **Feedback option.** With a new icon, **Submit Feedback**, you can now directly provide feedback, comments, and suggestions for preview features. This feature helps us gather valuable insights and improve our services based on your input.

Option to export data from the Cost optimization page. You can export the data in the **Cost optimization** page using data integration and ODATA queries. To export data, you can use on of the following options:

- Setup data integration - You can integrate Cost optimization data with Monitor Service API using which you can collect the data for troubleshooting and triaging the issues. For more information, see Integrations and data exports page.
- ODATA queries for cost optimization - You can use the available sample ODATA queries on the **Cost optimization** page to export data.

For more information, see Export data.

Webhook configuration using PowerShell SDK. The Webhook Configuration feature using PowerShell SDK allows administrators to create, modify, delete, and list webhook profiles. This

© 1997–2026 Citrix Systems, Inc. All rights reserved.

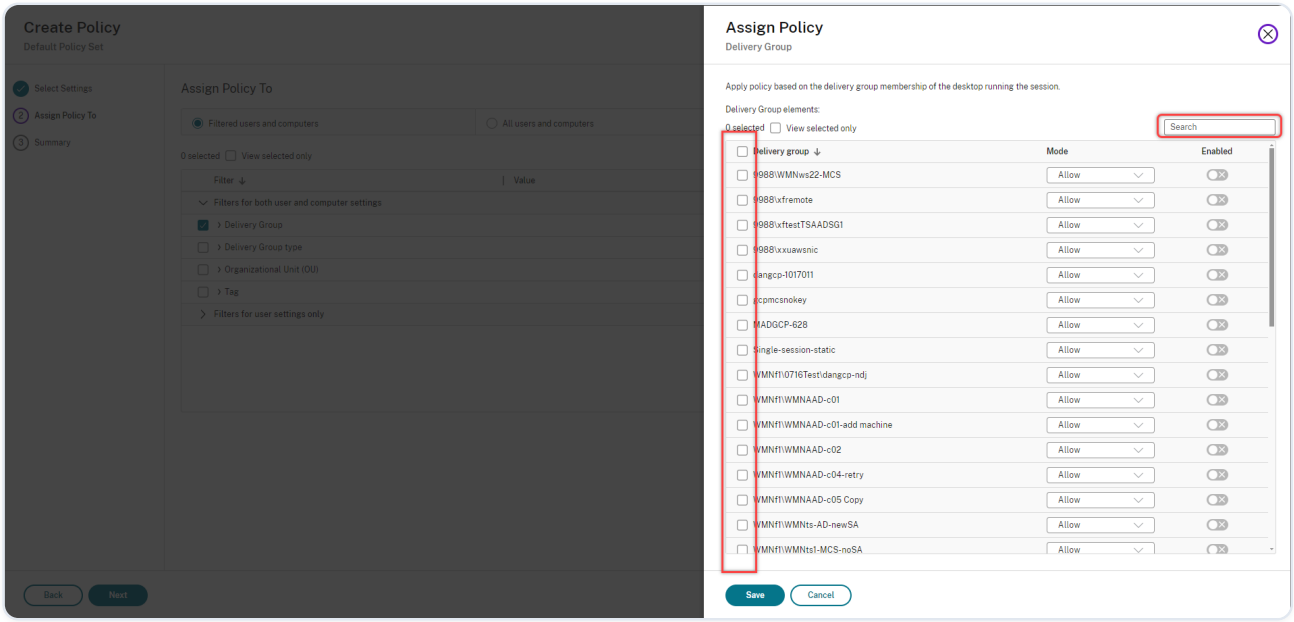
feature provides flexibility in configuring webhooks by allowing the specification of headers, authentication types, content types, payloads, and webhook URLs.

NOTE:

The supported payload format is text and the end user must enable text in their webhook.

For more information, see the Webhook configuration using PowerShell SDK documentation.

Enhanced policy assignment experience. You can now simplify your policy assignments in the **Policies** node with the new multi-selection and search functions. With those functions, you can view all objects of a selected type on the **Assign Policy** page and assign policy settings to multiple targets in fewer clicks. You can also use the search function to quickly filter and find specific objects, saving your time and reducing errors.



August 2024

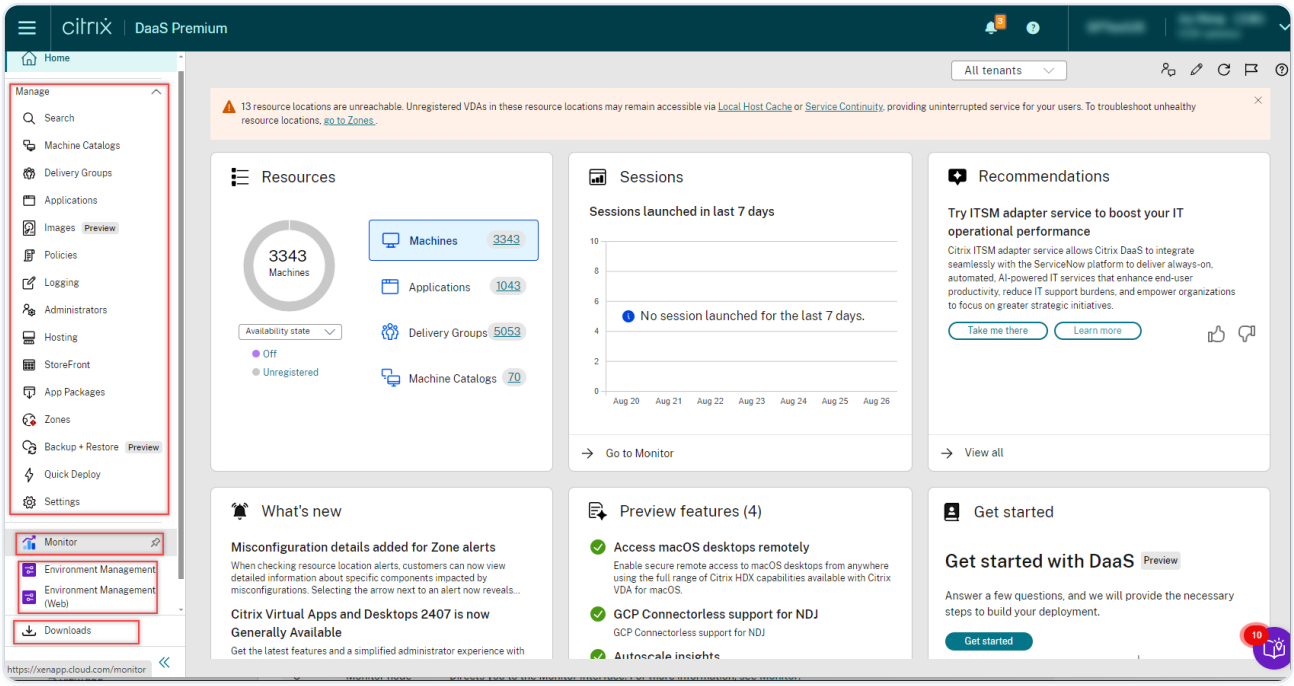
New and enhanced features

Redesigned DaaS navigation pane. We've revamped the DaaS navigation pane to streamline your management tasks:

- **Simplified navigation:** Reduced from two layers to one by moving the **Manage** and **Monitor** menus and the **Downloads** link from the top menu bar to the left navigation pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Centralized configuration:** All configuration-related nodes and menus are now located in the Manage section on the left navigation pane, consolidating items from the previous **Full Configuration** and **Quick Deploy** menus.
- **Reorganized Cloud services for machine management:** The **Environment Management**, **Environment Management (Web)**, and **Session Recording services**, previously under the **Manage** menu, are now at the same level as the **Manage** menu in the navigation pane.
- **Pin menus for quick access:** The newly added **Pin** function allows you to pin frequently used menus at the top of the navigation pane for quick access. You can reorder pinned menus by dragging them to desired places.



MCS creates ID Disks with GP3 volume type in AWS environment. Previously, in AWS environments, the Identity disks (ID) of VMs were of GP2 volume type. With this feature, MCS can now provision VMs with Identity disks of GP3 volume type. As GP3 volume type is the cheapest option offered by AWS, this feature minimizes cost.

The feature is applicable only to the VMs added to a new catalog and new VMs added to an existing catalog. Existing VMs created before this feature continues to have ID disks with GP2 volume type, unless the ID disk is reset.

Validate permissions on host connection in AWS. In AWS environments, you can now validate permissions on a host connection to do tasks related to creating and managing MCS machine catalogs. This implementation helps you to find out the missing permissions required for different scenarios such as creating, deleting, and updating VMs, power management of VMs, and EBS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

encryption, ahead of time so that you can avoid being blocked at critical times. For more information, see Validate permissions on host connection.

Create Custom Image from an existing Workspace Instance. This enhancement allows you to create a custom image from an already existing workspace instance. For more information, see Create Custom Image from an existing Workspace Instance.

Persist BDM storage type as standard SSD in Azure. Going forward, for Citrix Provisioning catalogs that are created using MCS in Azure, the BDM storage type is configured as standard SSD by default. This option is considered as a cost-saving measure and cannot be modified.

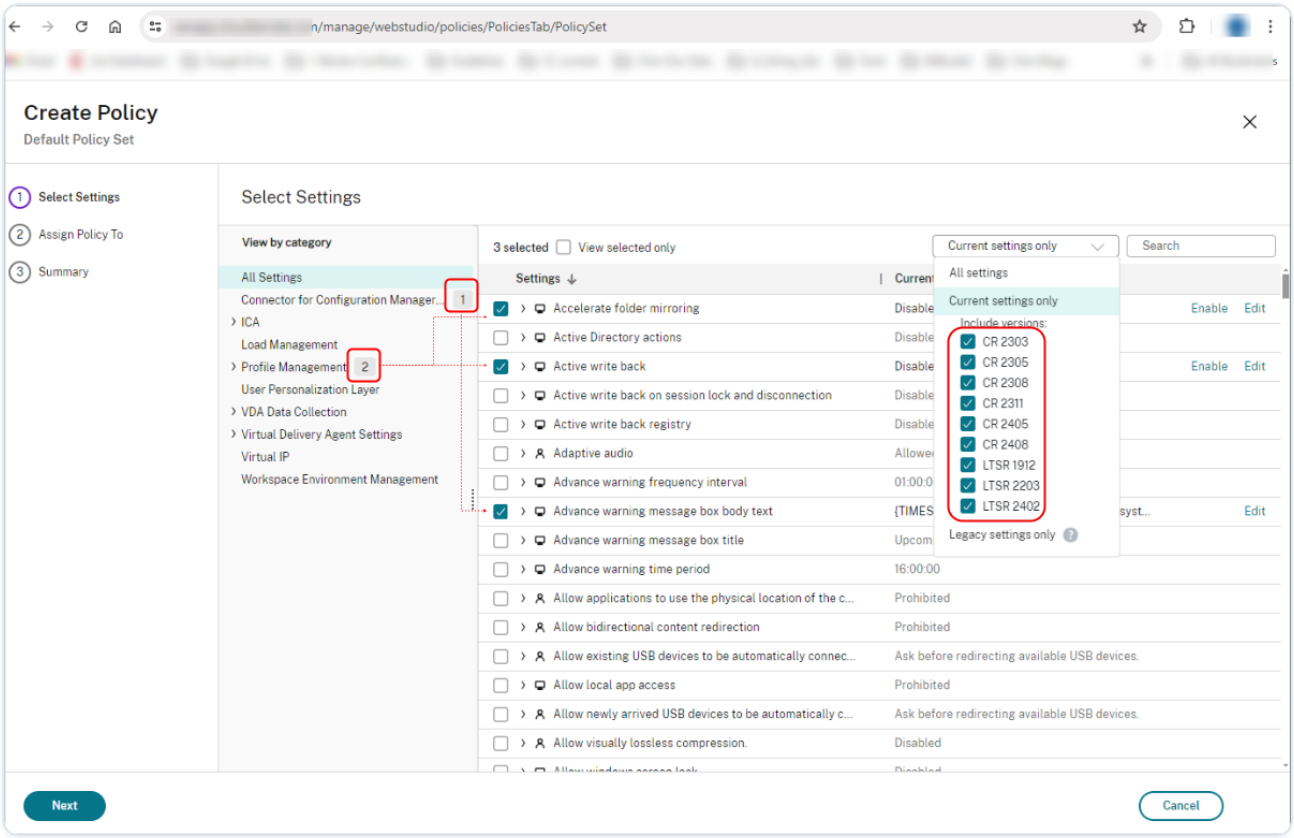
Customize the Home Page. You can now personalize the DaaS **Home** page by adding, removing, and repositioning its widgets to suit your needs better. This customization is specific to each administrator, ensuring a personalized dashboard experience. For more information, see Home page for the Full Configuration interface.

Misconfiguration details added for Zone alerts. When checking resource location alerts, you can now view detailed information about specific components impacted by misconfigurations. Previously, only general information was available on the **Troubleshoot** tab of the **Zones** node, making it difficult to address precise problems. With this enhancement, clicking the right direction arrow next to an alert reveals more specific details, enabling you to take targeted actions on misconfigurations. For more information, see Troubleshooting.

Policies UI improved for better user experience. We've enhanced the UI design for the **Policies** node to improve its overall usability and functionality. Detailed improvements include:

- **Full screen for creation and editing UIs.** Full-screen mode is now used for an improved and more efficient creation and editing experience on the **Policies** node.
- **Simplified setting filtering.** A dropdown list for supported VDA versions is now available under the **Current settings only** filter, allowing you to filter settings based on VDA versions.
- **Enhanced setting categorization.** When you select multiple settings, the number of settings chosen now appears next to the relevant categories and sub-categories in the left pane. This improvement helps you quickly identify the category and sub-categories to which each selected setting belongs, streamlining your policy management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Data caching for the Details tab on Full Configuration nodes. We've introduced data caching for the **Details** tab on all Full Configuration nodes. This enhancement significantly reduces the data load time for the **Details** tabs, improving the overall user experience.

Application usage monitoring charts on Dashboard. Now, Citrix Monitor helps you to monitor the usage of published applications. This feature is present on the Dashboard and contains curated charts to help the IT admins or application admins to gain insight into which applications are heavily used and the extent of their usage.

These charts comprise of the following data points for the last 24 hours:

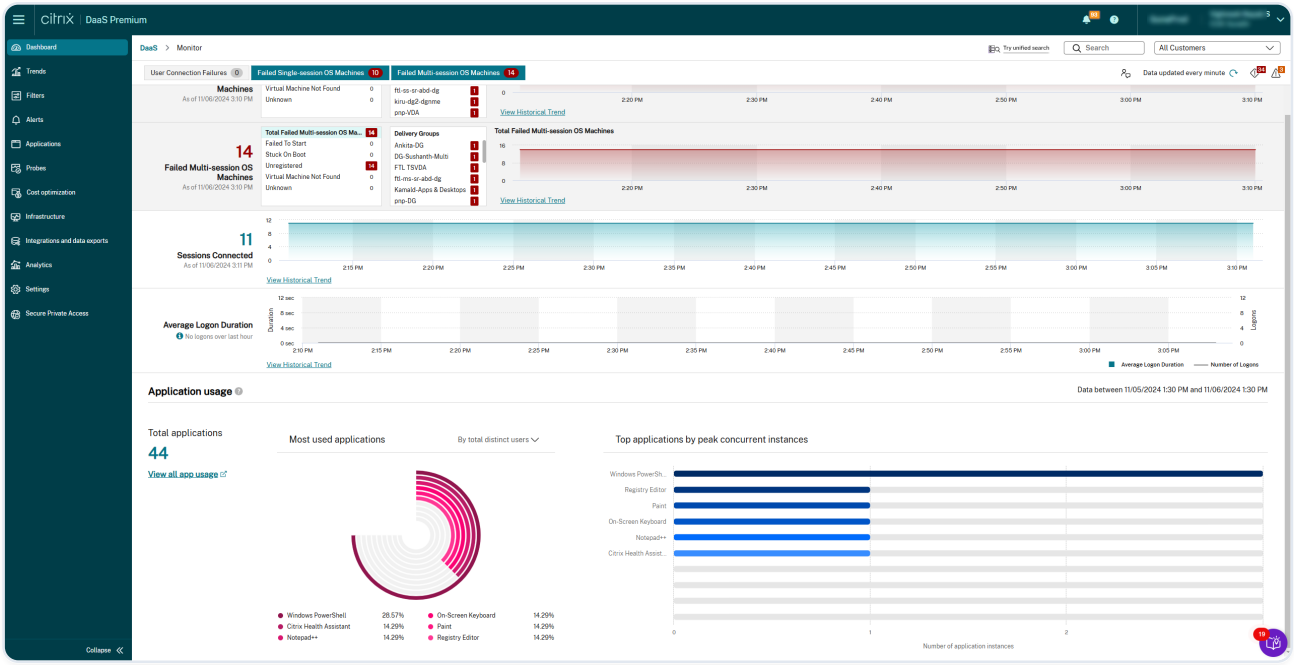
- Total number of applications in use
- Most used applications (limit 10) by total number of distinct users
- Most used applications (limit 10) by total number of application launches
- Top peak concurrent application instances

Through this visualization, customers can get visibility into the popular published applications to perform a Consumption versus Entitlement analysis to optimize on cost incurred on purchasing software licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

This feature is available only for the platinum-licensed sites.



For more information, see Application usage monitoring charts on Dashboard.

Option to view and filter session type and last boot time. Citrix Monitor now offers an option to add **Session Type** as a new column. The different session types available are desktop and application. You can also add **Session Type** as a new column by adding it at **Filters** > **Sessions** > **Choose Columns.** This is also added at **Trends > Sessions.**

Similarly, a new option to find out the **Last Boot Time** is added on the **Filters** > **Machines** section. You can also add **Last Boot Time** as a new column by adding it at **Filters** > **Machines** > **Choose Columns**.

Convert legacy MCS catalogs to machine profile-based catalogs in Azure and AWS. You can now convert non-machine profile-based machine catalogs to machine profile-based machine catalogs in Full Configuration for both Azure and AWS environments. This new capability allows you to upgrade legacy MCS catalogs to the recommended machine profile-based catalogs.

For more information, see:

- Convert legacy MCS catalogs in Azure to machine profile-based catalog
- Convert legacy MCS catalogs in AWS to machine profile-based catalog

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for backup VM sizes configuration. Public clouds can sometimes run out of capacity for a specific VM size. Also, if you use Azure Spot VMs, then the VMs are evicted at any time based on Azure's capacity needs. In such a case of insufficient capacity on Azure or a Spot VM power-on failure, MCS now falls back on the backup VM sizes.

You can provide a list of backup VM sizes using a custom property `BackupVmConfiguration`. MCS tries to fall back on the backup VM sizes in the order that is provided by you in the list. In case, MCS fails to fall back on all backup VM sizes provided, you get an error message. This feature is supported only for a catalog that uses a machine profile and is applicable to both persistent and non-persistent MCS machine catalogs. This feature is currently supported only for Azure environments. For more information, see Configure backup VM sizes.

July 2024

New and enhanced features

Configure required Azure host connection permissions. Previously, the host connection test validated whether the credential is good to connect to the hypervisor. The test did not perform validation on actual permissions that you might need to perform relevant MCS operations such as power management, VM creation, and many more.

With this feature, you can now easily configure all the minimum permissions required for a service principal or user account in Azure tied to a host connection to perform all MCS operations using an ARM template. This ARM template automates the following:

- Creation of an Azure Role with minimal permissions necessary for operations.
- Assignment of this role to an existing Azure Service Principal at the subscription level.

You can deploy this ARM template using the Azure Portal or PowerShell commands. For more information, see ARM Template for CVAD Operations.

Enhanced Performance Metrics panel. The **Performance Metrics** panel has an enhanced visualization of the historical data metrics. When you click the **Session Performance** tab, along with the last 15-minutes data, you can view the last 24 hours data for ICARTT and ICA Latency. This enhancement helps to reduce mean time for resolution by enabling admins to triage issues even though the session was terminated in the last 24 hours.

For more information, see Performance Metrics.

Integrations and data exports. Citrix Monitor now provides a new UI for integrations and data exports. This feature helps to improve the awareness of the various interfaces and third-party

© 1997–2026 Citrix Systems, Inc. All rights reserved.

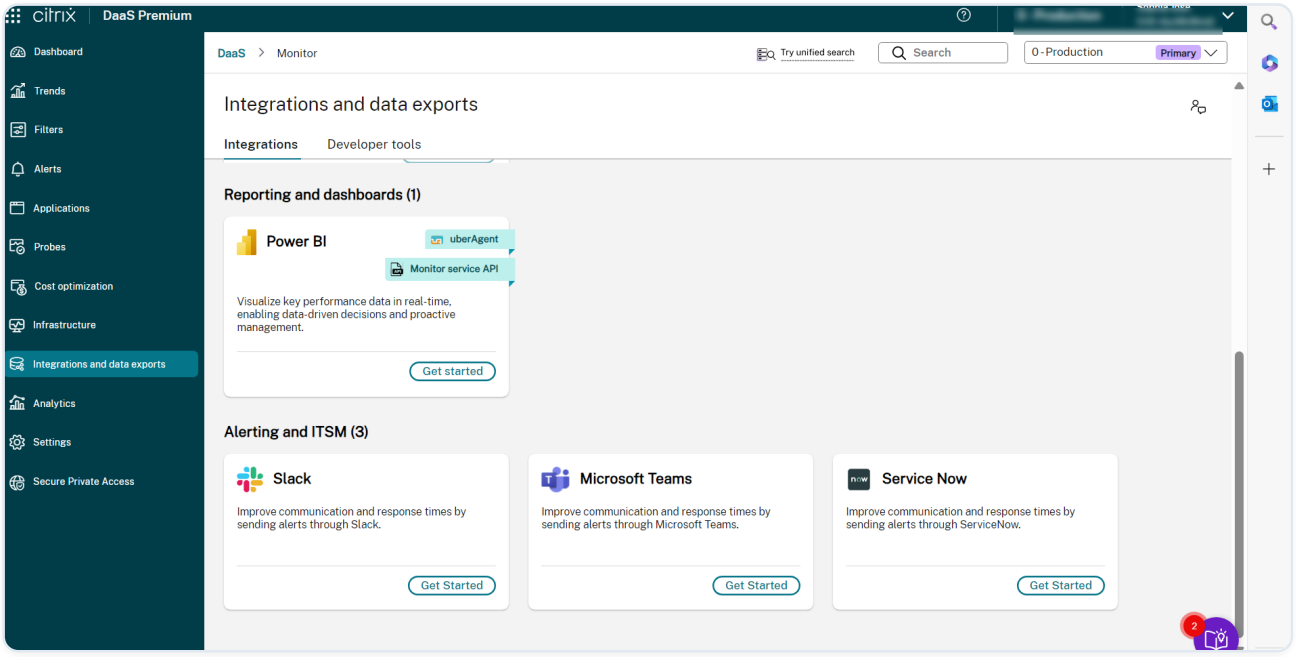
integrations available in Citrix Monitor. The newly introduced Integrations and Data exports page lists the following:

- Available integrations
- Supported developer tools

This page also describes the REST API set up for data exports and provides reference links to the guides and documents to get started with the integrations and developer tools.

Currently, Citrix Monitor is integrated with the Power BI observability. You can use this feature to export performance data and events from Citrix Monitor to Power BI using the REST APIs.

Click **Integrations and Data exports** from the left navigation menu. The **Integrations and Data exports** page appears.



For more information, see Integrations and data exports.

Enhancement on triaging user profile load issues. Citrix Monitor now supports the Profile Load duration and container metrics collection from Citrix Profile Management container and FSLogix container. This enhancement assists admin to receive comprehensive profile usage and performance data in user session reports. With this data you can identify and resolve issues with greater efficiency. For more information, see Profile load.

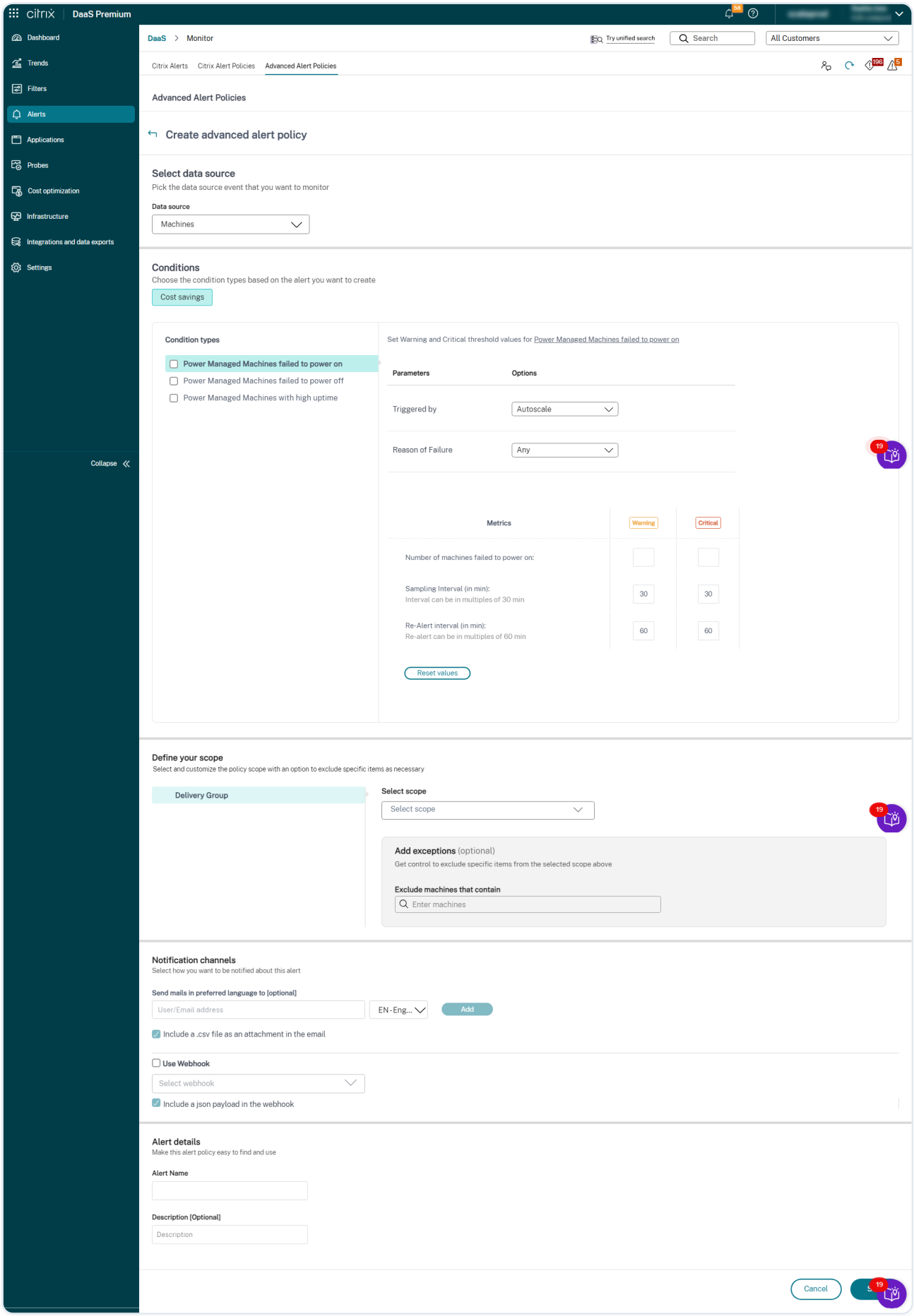
Advanced alert policies. The Proactive Notification and Alerting feature of the Monitor is enhanced to include a new alerting framework named **Advanced Alert Policies**. With this feature, you can create alerts by including granular details for each element or condition, thereby

© 1997–2026 Citrix Systems, Inc. All rights reserved.

enhancing the control over the alerts scope. Currently, these policies include alerts for cost savings and infrastructure.

This feature helps you to reduce excessive alerts which might lead to reduced responsiveness or effectiveness in addressing important issues. This policy helps to measure effectiveness of alert policies and engagement from admins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information, see Advanced alert policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhancements on alert content. The alerting feature of the Monitor is enhanced to include a CSV attachment and a JSON payload. With this enhancement, you can get alert details in a CSV attachment over email or as a JSON payload in case of a webhook. Using this CSV attachment and JSON payload, you can receive enriched content at a detailed level, aiding in the quick identification and resolution of issues.

Currently, this enhancement is available only on the following alerts:

- Machine uptime
- Failed power on actions
- Failed power of actions
- Unregistered machines (%)

For more information, see Enhancements on alert content.

Local Host Cache config sync failure alert monitoring. Local Host Cache allows user sessions to continue even if Cloud Connectors lose connectivity with Citrix Cloud. The cache used by Local Host Cache is regularly synchronized with the primary database to ensure up-to-date configurations when Local Host Cache mode is activated. You can learn more information about Local Host Cache and the config sync process at Local Host Cache. If the configuration sync fails more than three times consecutively, Citrix Monitor sends a warning alert to the administrator.

A predefined alert policy named **Local Host Cache - Config Sync Failure** has been introduced in Citrix Monitor to notify administrators about configuration sync failures. You can find the newly introduced policy on **Monitor** > **Citrix Alerts**. For more information, see Local Host Cache config sync failure alert monitoring.

Failed power on action and Failed Power off action alert. The Proactive Notification and Alerting feature of the Monitor is enhanced to include two new alerts, **Failed power on action** and **Failed Power off action** alerts based on the number of power-managed machines failed to power on or off in a delivery group. The new alert condition allows you to configure alert thresholds as the number of power-managed machines failed to power on or off in a delivery group.

For more information, see Failed power on action and Failed Power off action.

Infrastructure monitoring (Preview). Citrix Monitor now offers visibility into the operational health of Citrix Virtual Apps and Desktops components. This feature helps you to easily identify, troubleshoot, and resolve issues related to your infrastructure. Currently, the health of the Citrix Provisioning (PVS) and StoreFront components are monitored.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To support this feature, a new Windows executable named Citrix Infrastructure Monitor is introduced. This helps with the collection and transmission of relevant health metrics from PVS or StoreFront servers to Monitor.

This feature helps you to get critical monitoring data sets and proactive alerts with respect to PVS and StoreFront servers system metrics on a single console in Monitor. Data is collected every five minutes from the monitoring components to ensure the latest information.

This feature aims to enhance operational efficiency by offering proactive monitoring, detailed metrics, and automated alerts, ensuring your Citrix infrastructure runs smoothly and efficiently. For more information, see Infrastructure monitoring [Preview].

Infrastructure policy (Preview). This policy is introduced to create alerts related to the health of supported Citrix Virtual Apps and Desktops components.

Once the Infrastructure monitoring setup is completed, you can use the health data available in Monitor to configure alerts for any required component. Admins can set conditions, scopes, and notification mediums to receive important alerts through emails or a json payload through webhooks. The alerts raised are also available in the **Citrix Alerts** section for analysis and management.

As part if this policy, the following four new categories are introduced:

- Reachability
- Dependent services
- Impact
- Resource utilization

You can set different conditions and can modify the severity of the preceding categories as required in the **Critical** and **Warning** section. You can also schedule re-alert intervals for these alerts.

Conditions within each category can be set with the severity of Critical and Warning based on your organizational priorities. You can also schedule re-alert intervals for these alerts.

For more information, see Infrastructure policies (Preview).

Increased limit of replicas per image version in Azure. Azure has increased the maximum count of replicas for a gallery image single version to 100. With the increase in limit, you can now set the property `SharedImageGalleryReplicaMaximum` to a maximum value of 100 while

© 1997–2026 Citrix Systems, Inc. All rights reserved.

creating an MCS machine catalog using the Azure Compute Gallery image. For more information, see Configure Azure Compute Gallery.

Managing prepared images with the Images node. An **Images** node is now available in Full Configuration interface, that lets you prepare an MCS image (prepared image) from a single source image and deploy it across various MCS machine catalogs. This node facilitates complete image lifecycle management, enabling you to create image definitions, versions, and catalogs.

Images prepared using this node can only be used in Azure and VMware environments. For detailed information on image management, see Image management (Preview).

Alternatively, you can also create catalogs with prepared images using the **Machine Catalogs** node. For more information, see Creating machine catalogs.

Detailed misconfiguration report. The misconfiguration alerts that are exposed in the **Zones** node of the Full Configuration interface provide general information about a misconfiguration in the resource location.

With this enhancement, a new PowerShell cmdlet, `Get-ConfigMisconfigurationReport`, provides a detailed misconfigurations report in the zone. Added details include information such as which Connector is misconfigured, what is the current misconfiguration, and what is the recommended configuration. See Troubleshooting for the documentation on misconfigurations.

Introducing user and desktop display names in the Search node. To improve your troubleshooting efficiency, we've introduced two new columns on the Search node:

- **User Display Name** column on the **Sessions** tab. With this column, you can quickly identify sessions associated with a specific user.
- **Desktop Display Name** column on both the **Single-session OS Machines** tab and the **Sessions** tab. With this column, you can quickly identify the machine associated with a specific desktop.

Additionally, we've added corresponding filters for efficient searching. For more information about these two columns, see Machine actions and columns and Session actions and columns.

Modify desktop display names using Full Configuration. We've enhanced the **Machine Allocation** page for single-session OS static delivery groups by introducing a new column, **Display name**. With this addition, you can now modify desktop display names for machines assigned to users. For more information, see Manage user assignments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Options to troubleshoot when ICA RTT or Session Logon Duration data fails to populate. Previously, when EUEM service or UPM service failed to run, the reason for failure in getting the data related to ICA RTT or Session Logon Duration wasn't displayed. With this new feature, you can get the reason for failure and the corresponding solution for the failure. For more information, see Troubleshoot when ICA RTT or Session Logon Duration data fails to populate.

Support for Azure's nested virtualization. With this feature, if you configure the master VM with nested virtualization enabled, then all VMs in the MCS machine catalog created using that master VM have nested virtualization enabled. This feature is applicable to both persistent and non-persistent VMs. You can update an existing MCS machine catalog and existing VMs to have nested virtualization through image update.

Currently, only Dv3 and Ev3 VM sizes support nested virtualization.

For information on nested virtualization, see the Microsoft blog Nested Virtualization in Azure.

Support for inheriting labels from a machine profile source to the VMs and disks in GCP. With this feature, MCS machine catalog VMs and disks (Identity Disk, Write-cache Back Disk, and OS disk) can now inherit the labels of a machine profile source (GCP VM instance or instance template). You can use the labels to distinguish instances owned by different teams (for example, **team:research** and **team:analytics**), and further use it for cost accounting or budgeting.

For more information on labels, see the GCP document Organize resources using labels.

This feature is applicable to persistent and non-persistent MCS machine catalogs.

You can create a new MCS machine catalog, update an existing catalog, and update existing VMs to inherit the labels from a machine profile source.

For information on creating an MCS machine catalog, see VMs and disks with inherited labels.

Support for inheriting custom tags from machine profile to the provisioned VMs. You can now add the custom tags of an SCVMM VM to the MCS provisioned VMs along with the default `CitrixProvisioningSchemeId` tag. To add the custom tags to the provisioned VMs, you must use the SCVMM VM as a machine profile while creating or updating an MCS machine catalog. If you remove a VM from a catalog, then only the `CitrixProvisioningSchemeId` is removed from the tag. The custom tags are not deleted from the VM. This feature applies to a new MCS machine catalog and new VMs added to an existing catalog. For more information, see Create a catalog with a machine profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for on-demand capacity reservation in Azure. With this feature, you can create an MCS machine catalog of Azure VMs with on-demand capacity reservation using a machine profile (VM or template spec). This feature is applicable to persistent and non-persistent machine catalogs. You can update an existing machine catalog and existing VMs to have or remove on-demand capacity reservation.

For more information on Azure on-demand capacity reservation, see the Microsoft documentation On-demand Capacity Reservation. For information on creating and updating an MCS machine catalog with on-demand capacity reservation, see Create a catalog of on-demand capacity reservation VMs.

Support for placing WBC disk on the same storage location as OS disk. In XenServer, VMware, and SCVMM virtualization environments, MCS now places Write-back cache (WBC) disk on the same storage location as OS disk if you configure the available OS storage list the same as the available temporary storage list while creating a host connection.

This implementation helps to reduce the complexity in managing the OS and WBC disks. For creating a host connection, see Create a connection and resources.

Enhancement to Cost savings page. Cost savings page is enhanced with the following:

- **Estimated Savings** - The Estimated savings chart now includes additional filter options to view data for last 7 days and 30 days. It also shows savings in relation to the customer's account-specific pricing.
- **Filter by Tags** - Displays the tag of the machines that is configured in the Autoscale settings in a WebStudio. You can also filter the data based on the tagged machines. In this case, you will get only the tagged machines summary.
- **Average logon duration** - Displays the average time for a user to log on over the selected time duration.
- **Power managed machines** - The power managed machine chart now includes the hibernate state of the machine, which helps you to analyze how many machines are in hibernate state.

For more information, see Cost savings[Preview] section.

Get warnings messages for hibernation failure. You can now get warning messages using a PowerShell command `Get-ProvOperationEvent` in case of hibernation failure of MCS-provisioned and existing hibernation-capable VMs. For more information, see Get warnings messages for hibernation failure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Option to update write-back cache settings post creation for Machine Creation Service (MCS) catalogs in the hypervisors. You now have the option to update the memory and disk cache size of the write-back cache, when Machine Creation Service (MCS) Storage Optimization (MCSIO) is enabled, after the catalog is created for MCS catalogs in the hypervisors.

For more information, see:

- Create a machine catalog using a machine profile
- Create a catalog with a machine profile
- Create a machine profile-based machine catalog using PowerShell

Enhancement to Session Performance tab. The **Session Topology** section of the **Session Performance** tab is enhanced to include the following endpoint metrics which exists in the Citrix Workspace app for Windows:

- WIFI signal strength
- Throughput incoming and outgoing
- Network interface type
- Link speed

This enhancement helps to troubleshoot issues with respect to sessions quickly.

Diagnose historical user sessions . Citrix Monitor now displays the details of sessions in active, disconnected, or in terminated state. Previously, you could see the details of active sessions only. With this feature, helpdesk admins can troubleshoot issues with a session that was ended or in terminated state. The session details are available for last 24 hours and last 2 days. You can view the following details of an ended or terminated session:

- Machine Details panel - Displays the available details of the machine where the selected session was launched.
- Session Details panel - Displays the available details of the selected session.
- Session logon duration - Displays the information on the logon duration taken for the selected session. You can view the chart on time taken for brokering, machine start-up, hdx connection, authentication, GPOs, logon scripts, profile load on disk, and interactive session.

For more information, see Diagnose historical user sessions.

Machine uptime alert. The Proactive Notification and Alerting feature of the Monitor is enhanced to include a new alert, Machine uptime alert based on the uptime of a power managed machine in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a delivery group. For every delivery group, for which the machines crossed the threshold, you will get an attachment or webhook alert for that delivery group alone.

The new alert condition allows you to configure alert thresholds as the number of hours per day, hours per week, or hours per month for a machine is turned on in a delivery group.

For more information, see Machine uptime alert.

Published desktop name. Citrix Monitor now displays the published desktop name in the UI. This new field allows you differentiate among user groups within the same delivery group. You can also generate custom reports for these user groups. This new field is added to **Filters**, **Custom Reports**, or to **Machine Details** section of Citrix Monitor UI.

Infrastructure rightsizing. The **Infrastructure Rightsizing** page helps you to analyze the provisioning and sizing aspects of your delivery group based on the resources utilization. Based on this analysis, you can optimize the machine provisioning and sizing to match the utilization pattern. You can optimize your infrastructure cost by reducing spending on the unused resources. You can also choose to opt for lower CPU and memory specifications machines if the resource utilization is consistently lower than provisioned. You can optimize for performance by opting for a higher CPU and memory specifications machines if the resource utilization is consistency higher and see evidence of it impacting the session experience such as *Logon and ICARTT* metrics.

You can filter the Infrastructure rightsizing using the following:

- Delivery Group - You can filter for single session OS or multi session OS delivery groups
- Tags - Tags are the tag names applied to the machine. So, you can filter machines with the same tags. You can select multiple tags up to five tags. When you select multiple tags, you can filter for all the machines which have at least one of those selected machine tags applied.
- Time period - You can filter the data for last 24 hours, 7 days, and 30 days.

The Infrastructure rightsizing page offers:

- Insight in to the utilization details
- Summary of the resource utilization
- Trends on the resource utilization

Click the **Cost Optimization** tab from the left menu on the Home page. And then, click the **Infrastructure rightsizing** tab to access the **Infrastructure rightsizing** page.

You can also click the **Rightsize this delivery group link** from the **Infrastructure details** section in the **Cost Optimization** tab > **Cost savings** to access the **Infrastructure rightsizing** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Infrastructure rightsizing.

Local Host Cache activity dashboard. The new Local Host Cache dashboard under the **Trends tab** provides detailed information on user sessions and machines available during an outage on any Resource location or Zone. Administrators can use the details around number of machine registrations, reconnected sessions, and new sessions brokered to evaluate and audit activities while in Local Host Cache mode. The default selected data is for last 24 hours and for all zone and cloud connectors, with the ability to filter on time period, zone, and cloud connector. The Local Host Cache data is available for last 2 hours, 24 hours, 7 days, 1 month, and up to 90 days. For more information, see Available trends.

Specify CMEK global and regional keys from all projects. In Google Cloud environments, previously, you could only use customer-managed encryption key (CMEK) from within the same GCP project and the same region in which the hosting connection is created.

With this feature, you can now browse and use global or regional CMEK from all projects that are accessible to the service account. This feature enhances the flexibility to manage encryption keys. This feature requires extra permission for the following two service accounts:

- The service account of the current project with which the hosting connection is created.
- The Compute Engine Service Agent of the current project.

For more information, see Specify CMEK global and regional keys.

Decoupled Workspaces, allow userGroup assignment. Decoupled Workspaces now allows for a more flexible and independent management of users and their associated workspaces. It simply means, you can create deployments without associating any users to it and instead assign the users to a deployment later. For more information, see Create a deployment.

Support to import Workspace images type. You can now import Workspace images type to create a desktop experience for users. For more information, see Import an image.

Export function extended to all nodes in Full Configuration. You can now export records from the main view of any node in Full Configuration to a CSV file. Note the following:

- The **Export** icon is disabled while data is loading, except for the **Search** and **Applications** nodes.
- For nodes with the **Columns to Display** function, exported data includes only selected columns.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for adding notes for maintenance mode. You can now add notes when placing a machine, delivery group, or connection into maintenance mode. Those notes are visible in the **Maintenance reason field** of the Details pane, helping you and other administrators understand the reason for maintenance.

Data caching for the Zones and Policies nodes. We've introduced data caching for the **Zones** and **Policies** nodes. This enhancement significantly reduces the page load time when you navigate to a node, improving the overall user experience.

Option to update Write-back cache setting post creation for Machine Creation Service (MCS) catalogs in the Google Cloud Platform.

You now have the option to update the memory and disk cache size of the Write-back cache, when Machine Creation Service (MCS) Storage Optimization (MCSIO) is enabled, after the catalog is created for MCS catalogs in the Google Cloud Platform.

For more information, see Create a machine catalog using the Full Configuration interface.

Option for manually managing the service principal's role for Azure AD joined device management.

We've enhanced the **Enable Azure AD joined device management** option for greater flexibility. Previously, you had to sign in to Azure and allow Citrix to assign the **Cloud Device Administrator** role to the connection's service principal on your behalf. This design worked only when your Azure account had permission to grant this role.

With this enhancement, if your Azure account doesn't have the required permission, you can now choose Don't sign in to Azure when enabling Azure AD joined device management. This allows you to manually assign the role to the connection's service principal in the Azure portal.

For more information, see Enable Azure AD joined device management.

Install the FlexApp One agent. Liquidware has a package called FlexApp One. FlexApp One agent bundles the software applications along with their configurations and dependencies for easy distribution and deployment in a shareable file.

To support the discovery and publishing of Liquidware FlexApp One packages, install the FlexApp One agent on any VDA used for package discovery or launching. For more information, see Install the FlexApp One Agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 2024

New and enhanced features

Full Configuration: Support for provisioning VMWare VMs using machine profile. When provisioning VMWare VMs using Machine Creation Services (MCS), you can now select an existing template as the machine profile, letting the VMs within the catalog inherit settings from the selected template.

The inherited settings include:

- Tags placed on the template
- Custom attributes
- vSAN Storage policies
- Virtual hardware version
- vSphere Virtual TPM (vTPM)
- CPU count and core per socket
- NIC count

Create delivery groups exclusively for suspend-capable VMs using Full Configuration. We've introduced a new option in **Full Configuration > Create Delivery Group**, **Make suspend capability required for this delivery group**. This option enables you to create delivery groups that contain only suspend-capable VMs, facilitating your machine power management at the delivery group level. Note that this feature applies only to single-session OS VMs.

For more information, see Create delivery groups.

Enhanced Performance Metrics panel. The **Performance Metrics** panel has an enhanced visualization of the historical data metrics. When you click the **Session Performance** tab, along with the real time data, you can view the last 15 minutes data without waiting for the page load time. This enhancement helps to reduce mean time for resolution by enabling admins to be able to correlate multiple component performance metrics in a single view. For more information, see Performance Metrics.

Improved Session Logon view. - The new **Machine Start-up** option with the following sub-sections on the **Session Logon** tab on the **Filters** -> **User Details** page provides breakdown of the time taken to start a virtual machine during different phases:

- **Power on** - Displays the time taken to power on a virtual machine
- **Boot-up and registration** - Displays the time taken to boot up and register a virtual machine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The newly introduced collapsible button on the **Session Logon** page helps to collapse or expand the options on the **Machine Start-up** and the **Interactive Session**.

Along with the default **Logon Duration Phases** table options, which are **Session Logon Phase** and **Duration**, you can also choose the following columns on the **Session Logon** page:

- Start time
- End time
- Delivery Group's 7 Day Avg (sec)
- User's 7 Day Avg (sec)

You can also export the preceding data to a .CSV file.

The newly added columns **Power on** and **Boot up and registration** can be added to the **Logon Duration by User Session** table in the **Trends** -> **Logon Performance** > **Choose Columns**. You can also export the reports on the **Logon Performance** screen.

This enhancement helps to understand and easily troubleshoot issues related to logon duration. For more information, see Diagnose user logon issues.

Unregistered machines alert. The Proactive Notification and Alerting feature of the Monitor is enhanced to include a new alert, **Unregistered Machines (in %)** based on the percentage of unregistered machines in a delivery group. The new alert condition allows you to configure warning and critical threshold values as a percentage of unregistered machines in a delivery group. For more information, see Unregistered Machines (in %) section in the Alerts article.

Shared or Dedicated directory connections. You can now create directory connections using dedicated or shared tenancies. If dedicated tenancy is selected while adding a directory connection then the workspaces created are for single session desktops. If shared tenancy is selected while adding a directory connection then the workspaces created are shared. For more information, see: **Shared or Dedicated directory connections.** You can now create directory connections using dedicated or shared tenancies:

- If you select dedicated tenancy while adding a directory connection then the workspaces created are for single session desktops.
- If you select shared tenancy while adding a directory connection then the workspaces created are shared. For more information, see:
    - Create a directory connection
    - Import an image

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Create a deployment

Contextual App Protection. With this feature, the administrators can apply **App Protection Anti-Screen Capture** and **Anti-keylogging** control on devices and users contextually instead of having the controls always enabled or always disabled. This implementation helps you to enforce **App Protection Anti-Screen Capture** and **Anti-keylogging** only when required. For more information, see Step 7. App Protection and Manage app protection.

Enhanced default view settings for machine catalogs, delivery groups, and applications. We've introduced new default view options for Machine Catalogs, Delivery Groups, and Applications, offering greater flexibility and customization:

- **Default view selection.** Previously, those nodes defaulted to a folder view, which was suitable for organizations using folder-based management structures. With the introduction of a **Folder** icon on the action bar, you can now switch between folder view and list view as your preferred default view.
- **Improved folder view.** The **View all** toggle now retains your last selection when you sign back in. If previously turned off, it will remain off, with the root folder selected and the first-level sub-folders expanded.

Data caching for the StoreFront node. We've introduced data caching for the **StoreFront** node. This enhancement significantly reduces the page load time when you navigate to the **StoreFront** node, improving the overall user experience.

Improved user name search in machine catalog creation. We've enhanced the functionality for searching for administrators by user names during machine catalog creation. Key enhancements to the **Machine Catalog Setup > Enter Credentials** page include:

- **Domain specification:** A new option, **Domain**, is now available on that page, enabling you to narrow the search by entering the domain name or SID.
- **SamName search optimization:** Searches using SamName are now confined to the specified domain.

These enhancements make user searches faster and more efficient.

Simplified subnet updates for machine catalogs. Previously, to change the subnet settings of a machine catalog, you had to delete and recreate it. With this feature, you can now achieve the same functionality by editing the catalog. Note that only new virtual machines created under the catalog will be on the newly associated subnets. This enhancement reduces the need for catalog deletion and associated tasks. For more information, see Edit a catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for creating resource groups during Azure catalog creation (for PVS). Previously, when creating Azure catalogs using Full Configuration, you had to create the resource groups using PowerShell commands. With this feature, you can now seamlessly create a resource group as part of catalog creation in Web Studio. This enhancement simplifies the overall creation workflow. For more information, see Create a Citrix Provisioning catalog using the Full Configuration Interface.

May 2024

New and enhanced features

Secure HDX (Preview). You can now use this feature to prevent any network elements in the traffic path from being able to inspect the HDX traffic. For more information, see Secure HDX.

Azure GPU hibernation support (Preview). You now have the option to support hibernation for Azure machine SKUs that support GPU. For more information on supported VM sizes, see the Microsoft documentation.

Citrix Provisioning catalogs support for hybrid Azure AD join extended to Full Configuration. When you create a Citrix Provisioning catalog, the **Hybrid Azure Active Directory joined** identity type is now available on the **Machine Catalog Setup > Machine Identities** page. With this new option, you can create hybrid Azure AD joined machines through Citrix Provisioning. For more information, see this Citrix Provisioning article.

Enhancements to Full Configuration contextual help. We've redesigned the help panel to provide a more informative experience, offering targeted information for each node within Full Configuration. By clicking the Help icon on any node, you can now access a comprehensive set of resources aimed at providing a one-stop learning experience, helping you better understand related features:

- Access key documents specifically related to the selected node.
- Stay informed about service updates including Citrix Roadmap, Known issues, Limits, System requirements, and What's new features.
- Access expanded resources such as Citrix Blogs, Citrix Community, Citrix Feature Explained, Citrix Product Documentation, Citrix Support, and Developer Documentation.

Enhanced configuration logging: tracking membership changes for delivery groups. With this enhancement, configuration logging now captures and displays user and group IDs added to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

or removed from delivery groups. To view configuration logs, go to **Full Configuration > Logging > Events**.

Customize the tab order on the Search node. You can now customize the order of tabs on the **Search** node according to your usage patterns, enhancing the browsing experience. To do so, click the three-dot icon next to the tabs, drag the tabs to your preferred order, and then click **Apply**.

Data caching for the Machine Catalogs node. We've introduced data caching for the Citrix DaaS **Machine Catalogs** node. This enhancement significantly reduces the page load times when you navigate to the **Machine Catalogs** node, improving the overall user experience.

Support for creating Citrix Provisioning catalogs using MCS PowerShell commands in VMware. You can now create Citrix Provisioning catalogs using MCS PowerShell commands in VMware.

This implementation provides you the following advantages:

- A single unified API to manage both MCS and Citrix Provisioning catalogs.
- Have new features for Citrix Provisioning catalogs, such as, identity management solution, on-demand provisioning, and so on.

For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

Failure Detection and Mitigation in VDA Upgrade Service During the VDA upgrade process (Preview). Our service now incorporates advanced detection mechanisms. If any issues are detected that could potentially lead to the failure of the VDA IPU, rendering the VDA unusable, the service will take proactive measures. It will cease to update additional machines and gracefully exit the current workflow. This proactive approach aims to minimize the impact and ensure a smooth experience, even in the event of unexpected challenges, reducing the potential blast radius of any issues encountered. For more information, see Failure Detection and Mitigation in VDA Upgrade Service

Support VDA Updates from a local file share that VDAs have access (Preview). With Enhanced VDA Installer Access Control, you can now have greater flexibility and control over which VDAs can connect and retrieve necessary download MSIs without worrying about granting network access for VDAs to fetch updates from the Citrix Managed Azure CDN. This allows you to enforce stricter network rules while ensuring seamless access to essential updates. For more information, see Support VDA Updates from a local file share that VDAs have access

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Full Configuration support for delivering packaged applications to single-session static desktops and office PCs. With this enhancement, you can now deliver packaged applications to all types of desktops using Full Configuration. Benefits of delivering packaged applications to *single-session static* desktops include:

- Applications are available on the VDA at sign-in and not staged on demand through Workspace or StoreFront.
- Improved launch time when accessing the packaged applications.
- Facilitates maintenance of the packaged applications independently, separate from the VDA's base image.

To deliver packaged applications to desktops, add those applications to the delivery groups using these ways:

- Add applications during delivery group creation.
- Add applications to an existing delivery group using one of these entries: **Delivery Groups > Add Applications > Applications**, **Applications > Properties > Groups**, or **App Packages > Packages > Add Delivery Groups**.

For more information, see Create delivery groups, Manage delivery groups, and Add applications to delivery groups.

Full Configuration support for delivering packaged applications in FlexApp format. In **Full Configuration > App Packages**, you can now upload FlexApp packaged applications to Citrix Cloud, and deliver them to your users. For more information, see App packages.

OData pagination. Monitor enhances the limit of OData pagination. All OData v4 endpoints return a maximum of 1000 records per page with a link to the next 1000 records in the response. Because every page returns large data sets, you can get the same amount of total data with lesser OData queries. Thus this feature reduces time to get total data and thus improves the user experience. For more information, see Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud documentation.

Support for creating and managing Azure confidential VMs using Full Configuration. Azure confidential VMs provide a strong, hardware-enforced boundary to help meet your security needs. With the Full Configuration user interface, you can now create and manage confidential VMs on Azure. For more information, see Azure confidential VMs (Preview).

Support for displaying client IPs in configuration logs. In **Full Configuration > Logging > Events**, you can now view IP address details in logs, facilitating tracking of action origins. To show

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the IP address column in the main view, click the **Columns to Display** icon in the top right of the logs, and then select **Client IP**. For more information, see View configuration log content.

Support for capturing additional properties using machine profile source in AWS. In AWS environments, with this enhancement, you can now create or update a machine profile-based catalog to include the following:

- Capture CPU options, tenancy type, and hibernation capability from the machine profile source while creating an MCS machine catalog.
- Change the tenancy type of the machine profile source while editing an MCS machine catalog. This functionality is applicable only to the new VMs added to the catalog.
- Change the hibernation capability of the machine profile source while editing an MCS machine catalog. This functionality is applicable only to the new VMs added to the catalog.

The machine profile source can be a VM or launch template version. This feature is applicable to both persistent and non-persistent catalogs.

For more information, see Create a machine profile-based machine catalog using PowerShell.

Repair the identity information of active computer accounts in AWS. In AWS environments, you can now reset the identity information of active computer accounts that have identity-related problems. You can choose to reset only the machine password and trust keys, or reset all configuration of the identity disk. This implementation is applicable to both persistent and non-persistent MCS machine catalogs. Currently, the feature is supported only for AWS, Azure and VMware virtualization environments. For more information, see Repair the identity information of active computer accounts.

Support for encrypting ID disk of an MCS machine catalog VMs in AWS. Previously, in AWS environments, MCS allowed the encryption of only the OS disk of the provisioned VMs. With this feature, you can now encrypt the ID disk in addition to the OS disk. This functionality allows you to use AWS KMS keys (Customer managed key and AWS managed key) to perform cryptographic operations on the disks attached to a VM.

For encryption of OS and ID disks, configure one of the following:

- Use a master image that is encrypted (for example, an AMI created from an instance or snapshot that contains a root volume encrypted with KMS key)
- Use a machine profile source (VM or launch template) that contains an encrypted root volume.

For more information, see Encrypt OS and ID disks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure security groups per network interface in AWS. When editing a host connection for AWS environments, you can now configure the maximum number of security groups allowed per elastic network interface (ENI) using a PowerShell command. Therefore, if you increase your security groups per network interface quota, you can configure the same value for the hosting connection. For information on configuration, see Configure security groups per network interface.

Cost optimization . The **Cost Optimization** page provides a visual representation of infrastructure savings accrued over a selected period and forecasts expected savings for the remaining days. By analyzing machine usage and sessions, this page helps you to identify achieved savings and opportunities for cost reduction. This page offers:

- Insight into the optimization of infrastructure costs
- The amount saved
- Information on a range of scenarios that might result in exceeding projected costs
- Potential opportunities for identification and strategic planning to realize infrastructure cost savings

The **Cost Optimization page** includes **Estimated savings** and **Autoscale savings report**.

The **Estimated savings** helps to evaluate the efficient utilization of infrastructure resources. The cost savings are displayed in either US dollars or as a percentage of the cost incurred. You can view the results for the last 3, 6, and 12 months. The **Estimated savings** graph displays the following:

- Estimated savings - Displays the amount of savings achieved in infrastructure for the selected duration
- Power managed machines - Displays the total number of power-managed machines.
- Projected savings - Displays how much infrastructure savings can be done for the remaining duration

The **Autoscale savings report** displays information about the delivery group for which the Autoscale is configured and enabled. This report is applicable only for power-managed machines. For more information, see the Cost Optimization page.

Inspect machines with recent power actions. You can now inspect machines with the status of the success and failed power actions. This feature helps you to analyze the following:

- Power on failure which causes user issues
- Power off failure which increases cost

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Data is available only for the power-managed machine. Data is not available for the power actions taken before the feature was supported.

You can view the power action status of the machines using the following ways:

- From **Filters** -> **Machines** tab. In this case, by default the **Power Action Time** and the **Power Action Result** columns are visible. You can also select the columns that you want to visible.
- From **Cost Optimization** tab. In this case, the default filter is **Power Action Triggered By** is set to *Autoscale* and the **Power Action Result** is set to *Failed*.

With this feature, you can view the details of the power action controls. For example, you can view who triggered the action, which action changed the power state, the reason for failure, and the time when the action is completed. You can also export these details.

For more information, see Inspect machines with recent power actions.

April 2024

New and enhanced features

Support for newer version of Microsoft Teams. Citrix Monitor now supports Microsoft Teams version 2.1 or earlier.

Change disk encryption in Azure. With this feature, you can now change the disk encryption in Azure virtualization environments. You can do the following:

- Create an MCS machine catalog with a disk encryption set (DES) that is different from the master image DES.
- Change the disk encryption type from one DES key to another DES key of an existing MCS machine catalog and existing VMs.
- Update an MCS machine catalog and VM that was not previously CMEK enabled to have customer-managed encryption key (CMEK) encryption (DES), disk encryption at host, or double encryption.
- Update an existing MCS machine catalog and VM to be non-encrypted that was previously encrypted.
- Enable disk encryption with private endpoint (an MCS machine catalog that used a host connection enabled with `ProxyHypervisorTrafficThroughConnector`).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Change disk encryption.

Support for modifying the page file settings. With this feature, you can modify the page file settings of the newly added VMs to an existing catalog without updating the master image. Currently, this feature is applicable to only Azure environments.

To modify the page file settings, you need VDA version 2311 or later. You can modify the page file settings using the PowerShell commands. For more information on modifying the page file settings, see Modify page file settings.

Check for multiple NICs in VMware. In VMware environments, we have introduced various pre-flight checks when the hosting unit and machine profile template have multiple networks, and the `-NetworkMapping` parameter is used in the `New-ProvScheme` and `Set-ProvScheme` commands. For more information on the pre-flight checklist for multiple NICs, see Check for multiple NICs.

Support for creating Windows 11 VMs in GCP. You can now create Windows 11 VMs in GCP. If you install Windows 11 on the master image, then you must enable vTPM during the master image creation process. Also, you must enable vTPM on the machine profile source (VM or instance template).

This feature is applicable to:

- Persistent and Non-persistent MCS machine catalogs.
- Only sole-tenant node group.

For information on creating Windows 11 VMs on the sole-tenant node, see Create Windows 11 VMs on the sole-tenant node.

Virtual channel allow list support for environment variables. You can now use system environment variables in the trusted processes' path. For more information, see Using system environment variables.

Deprecated features in Full Configuration. The following features and settings have been deprecated in Full Configuration:

- Azure environments:

  Provisioning VMs using a master image from a different region has been deprecated. We recommend using Azure Compute Gallery to replicate the master image to the region where the VMs will be created.

- AWS environments:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The option **Apply machine template properties to virtual machines**, on the **Machine Catalog Setup > Machine Template** page, has been deprecated. We recommend using machine profiles to specify machine properties for VMs instead.

- All hypervisor and cloud service environments:

  Configuring the write-back cache with only a disk cache and no memory cache has been deprecated. We recommend setting the memory cache size to a value greater than zero.

Enhanced service disruption experience in Full Configuration. To enhance your experience during service disruptions, we've improved the notification content on the Full Configuration page. With this enhancement, you can now gain a clearer understanding of service disruptions, such as the causes, steps to enable service, and estimated enablement times. This enhancement covers the following service disruptions:

- Service enablement requests for first-time use
- Service pauses caused by prolonged inactivity
- Service outages caused by DaaS unavailability

Data caching for the Hosting node. We've introduced data caching for the Citrix DaaS **Hosting** node. This enhancement significantly reduces the page load times when you navigate to the Hosting node, improving the overall user experience.

Support for HDX Plus for Windows 365 Cloud PCs and Azure Virtual Desktops. Monitor now supports HDX Plus for Windows 365 Cloud PCs and Azure Virtual Desktops (AVD). For more information, see Troubleshoot Machines.

VDA environments with proxies for internet and URL filtering (Preview). You can now use the VDA Upgrade Service to update VDAs when you have proxies for internet connectivity and web filtering. The proxy configured in policy takes precedence over the proxy configured in registry. For more information, see Install VDAs. Also, refer to the list of urls that need to be white listed in the proxy.

Cloud Build Service Account Change. GCP is introducing changes to Cloud Build Services's default behavior and use of service accounts in new projects created after April 29, 2024. For more information, see Cloud Build Service Account Change. However, your existing Google projects and Citrix catalogs are not affected by this change. For more information, see:

- Configure and update service accounts
- Required GCP permissions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

March 2024

New and enhanced features

Dynamic Session Recording. You can now record the current active session using the Session Recording controls from the **User Details** screen without the need to re-establish the session. This feature enables quicker and effective troubleshooting of session experience-related issues faced by users. This is useful to debug issues that are difficult to reproduce.

For more information about Dynamic Session Recording, see the Session Recording service article.

Enrollment tool to register VDAs using WebSockets to machine catalogs. You can now use this enrollment tool to securely register your non-domain joined VDAs to machine catalogs. This feature provides the benefits of using only the TLS port 443 for communication from VDA to the Delivery Controller and removing port 80 traffic. For more information, see Enroll machines to catalogs using the WebSocket VDA enrollment tool.

Full Configuration: Support for updating more Azure VM settings using machine profiles. With Full Configuration, you can now update a wider range of settings for MCS-provisioned Azure VMs through machine profiles, which include:

- Machine size
- License type
- Availability Zone
- Dedicated Host Group ID

After you update the machine profile, Full Configuration compares the current settings with the new ones. If differences exist, you'll be prompted to confirm which to apply. This design ensures transparent and efficient VM setting updates.

Full Configuration: Support for Changing write-back cache properties for MCS-provisioned Azure VMs. For Azure VMs provisioned using Machine Creation Services (MCS), you can now change their write-back cache (WBC) properties using Full Configuration, such as **Disk cache size**, **Memory cache size**, and **Enable storage cost saving**. In addition, when you select a new machine size or machine profile for those VMs, Full Configuration validates WBC settings to prevent conflicts, such as exceeding the memory limit of the new selection. If conflicts occur, you'll be prompted to re-configure WBC settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 2024

New and enhanced features

Suspend VMs from the Workspace interface. You can now suspend persistent VMs with active sessions from the Workspace user interface. This enhancement offers the following benefits:

- Resume the system from where you left off.
- Faster launch time compared to a stopped deallocated machine.
- Cost-effective and energy efficient.
- Efficient resource allocation using the Autoscale feature.

New Machine Creation Services (MCS) Storage Optimization (MCSIO) support: You now have the option for the Image Portability Service to add or remove MCSIO when you prepare an image for the MCS provisioning. For more information, see Automate VDA configuration.

Probes Overview enhancements: A summary of the Probe Metrics and the Probe Failure Stages in now available in the **Probe** > **Overview** page. The Probe Metrics shows the count of Scheduled, Failed, Skipped, and Successful runs. The graphical representation of the failure stages helps analyze the stages in which most failures have occurred. This information helps to quickly troubleshoot the probe results. For more information, see the Application and Desktop Probing article.

Image information on the Machine Catalogs page. You can now view the following image information through the **Template Properties** of the machine catalog:

- Operating system
- Machine identity service
- Machine Creation Service storage
- Filepath for `pagefile.sys` for Azure deployments

This enhancement provides better clarity on the image information and ensures that the administrators have all the information about the machine catalog in one place.

Full Configuration support for VDA enrollment token management. Token-based VDA enrollment reduces the load on Cloud Connectors and decreases potential failure points, ideal for the use cases where you prepare the machines using non-Citrix Provisioning technology. With Full Configuration, you can now generate and manage enrollment tokens for non-Citrix-provisioned

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDAs, streamlining enrollment token-based deployments. For more information, see Generate and manage enrollment tokens.

PowerShell logging. In Full Configuration, you can now view the PowerShell commands corresponding to your daily UI actions. This feature helps you gain insights into the underlying PowerShell commands for learning purposes. To view the PowerShell logs, go to **Logging > PowerShell**. For more information, see Configuration logging.

Enable Local Host Cache (LHC) for single-session pooled VDAs using Full Configuration. By default, single-session pooled VDAs provisioned using MCS or Citrix Provisioning are unavailable when in LHC mode. With Full Configuration, you can now override this default behavior on a per delivery group basis, making those VDAs available for new connections during LHC. For more information, see Create delivery groups and Manage delivery groups.

Citrix Hypervisor™ rebranded to XenServer in Full Configuration. In line with our rebranding strategy, we've updated all instances of Citrix Hypervisor within Full Configuration to XenServer.

End-to-end Network Hop view. End-to-end network hop view is the next step towards enhancing troubleshooting workflows in Citrix Monitor. The **User Details** > **Session Performance** > **Session Topology** section provides a visual representation of the end-to-end network hop view for connected HDX sessions. The in-session path helps understand the components involved in the session path with their metadata, the link between the components, and the applications published on the VDA. The Session Topology helps the data flows and to identify the specific hop that might be bringing in performance issues.

In addition, ICA Latency and ICA RTT measurements are displayed for the session when it is in a connected state. For more information, see End-to-end Network Hop view.

Use Disk Encryption Set ID (DES ID) of the master image to encrypt all the disks of catalog VMs. In Azure environments, previously, the Disk Encryption Set ID (DES ID) of an MCS machine catalog was derived from a machine profile or custom properties. With this feature, a machine catalog can also derive the DES ID from the master image to encrypt all the disks of the VMS in a catalog.

Update MCS tags to detect orphaned resources after migration. When you migrate from on-premises configuration to a cloud site, or from your cloud configuration to another cloud site, the orphaned resources aren't detected correctly because of the old site id tag. With this feature, using a PowerShell command, you can update the MCS site id tags of a persistent catalog, after migration so that orphaned resources can be detected correctly. Currently, this feature is applicable

© 1997–2026 Citrix Systems, Inc. All rights reserved.

to Azure. For more information, see Update MCS tags to detect orphaned resources after migration.

Validate configuration before creating an MCS machine catalog. With this feature, you can now validate configuration settings before creating an MCS machine catalog using the parameter `-validate` in `New-ProvScheme` command. After you run this PowerShell command with the parameter, you get an appropriate error message if there's an incorrect parameter used or a parameter has conflict with another parameter. You can then use the error message to resolve the issue and successfully create an MCS machine catalog using PowerShell.

Currently, this feature is applicable to Azure, GCP, and VMware virtualization environments. For more information, see Validate configuration before creating an MCS machine catalog.

Support for copying tags from a machine profile source to a VM in AWS. With this feature, in AWS virtualization environments, you can copy tags on NICs, and disks (Identity disk, write back cache disk, and OS disk) that are specified in the machine profile to newly created VMs in an MCS machine catalog. You can specify these tags in any of the machine profile sources (AWS EC2 instance or AWS launch template version). This feature is applicable to persistent and non-persistent machine catalogs and VMs. For more information, see Copy tags on VMs.

SCVMM support for machine profile. With this feature, you can now use a machine profile to create and update an MCS machine catalog in System Center Virtual Machine Manager (SCVMM) environments. You can also enable nested virtualization and vTPM. For more information, see Create a catalog with a machine profile.

Azure support for using spot VMs with MCS. Azure Spot VMs allow you to take advantage of Azure's unused computing capacity at a significant cost savings. However, due to its eviction policy, Azure Spot VMs are good for only some non-critical applications and desktops.

With this feature, you can create an MCS machine catalog of Azure Spot VMs using a machine profile (VM or template spec). You can update an existing catalog to have Azure Spot VMs as the newly created VMs or switch to have standard Azure VMs. You can also update existing VMs to be Azure Spot VMs. For more information, see Create a catalog using Azure Spot VMs.

Support for capturing diagnostic settings from a machine profile. In Azure environments, MCS now supports capturing of diagnostic settings on VMs and NICs from a machine profile while creating or updating an MCS machine catalog, or updating existing VMs. Therefore, with this implementation, the diagnostic data can be seamlessly transmitted to designated Azure destination endpoints, such as Log Analytics workspaces or Event Hubs, for in-depth analysis and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

visualization. For more information, see Capture diagnostic settings on VMs and NICs from a machine profile.

MCS support for managing different versions of a machine catalog. With this feature, you can manage the configuration versions of a machine catalog using PowerShell commands. Each configuration change using the `Set-ProvScheme` results in a new configuration version. You can:

- See the list of versions.
- Use any previous version to update a machine catalog.
- Manually delete a version if it isn't used by a VM.
- Change the number of maximum versions to be retained by a machine catalog.

For more information, see Manage versions of a machine catalog.

Publish App-V, MSIX and MSIX app attach packaged applications on single-session and shared desktop VDAs. You can now access packaged applications, for example, App-V, MSIX, and MSIX app attach on the single-session and shared desktop VDAs. This enhancement ensures that the packaged applications are readily available to use when you sign in. This feature facilitates faster launch of packaged applications and improves your experience significantly by bringing it closer to accessing a locally installed application. For more information, see Publish packaged applications on single-session or shared desktop VDAs.

Play back live and recorded sessions: Citrix Monitor now supports playing back recorded and live user sessions that are recorded using the Session Recording service. You can quickly understand the session-related issues encountered by the user from the replay. With this feature, you get ready access to recordings along with session-related metrics within the Monitor console. It helps corelate the issues discovered in the recordings with the performance metrics. It eliminates the requirement of searching for recordings across multiple session recording servers or looking for third-party apps to view the recordings.

This feature requires VDA and the Session Recording server version 2308 or later.

Monitor stores the recordings in a centralized repository and displays them on the **Session Selector** modal. The **Sessions with recordings** link displays the recordings of sessions that were active during the last 24 hours or the last 2 days. The recording is played back on a new tab using the Citrix Session Recording playback server.

For more information, see Record sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Teams Optimization: Monitor displays the status of HDX optimization available for Microsoft Teams. The new **Microsoft Teams Optimization** can be viewed in the **User Details** page > **Session Details** panel. Monitor displays the status of the Microsoft Teams optimization only if Microsoft Teams is run as a published app or inside a published desktop. This enhancement provides administrators with visibility to enable troubleshooting of session performance issues on Microsoft Teams reported by users. For more information, see Troubleshoot user issues.

User interface improvements: The Citrix Monitor user interface is now refreshed with a modern look and feel. The new and improved user interface provides easier navigation and better data representation. The improved experience is intuitive and designed to easily comprehend the data required to monitor and troubleshoot a Citrix session.

Optimal screen resolution: The recommended optimal screen resolution for viewing the Citrix Monitor is updated to 1440 x 1024.

January 2024

New and enhanced features

Enhanced bidirectional content redirection configuration Previously, configuring bidirectional content redirection involved managing three distinct policies: Allow bidirectional content redirection, Allow redirection of URLs to VDA, and Allow redirection of URLs to the Client. These policies require configurations on both the server side (configured in **DaaS > Full Configuration**) and the client side (configured through Group Policies). Starting with this release, we have consolidated all three policies into a single, unified policy. It not only simplifies and enhances the configuration process but also eliminates the requirement for client-side configurations. For more information, see Bidirectional content redirection configuration.

Support for restarting and shutting down single-session machines from the Search node's Sessions tab. On the **Sessions** tab of the **Search** node, you can now search for user sessions in an unhealthy state and seamlessly restart or shut down the associated single-session machines within the same tab. This feature enhances efficiency, enabling prompt action on identified session issues within a single interface.

Support for accessing Global App Configuration Service from Full Configuration. We've provided action items in the Full Configuration interface to link you to the Global App Configuration Service. With this integration, you can easily access Global App Configuration for managing end-user settings through Full Configuration.

To access this service from Full Configuration, you have two options:

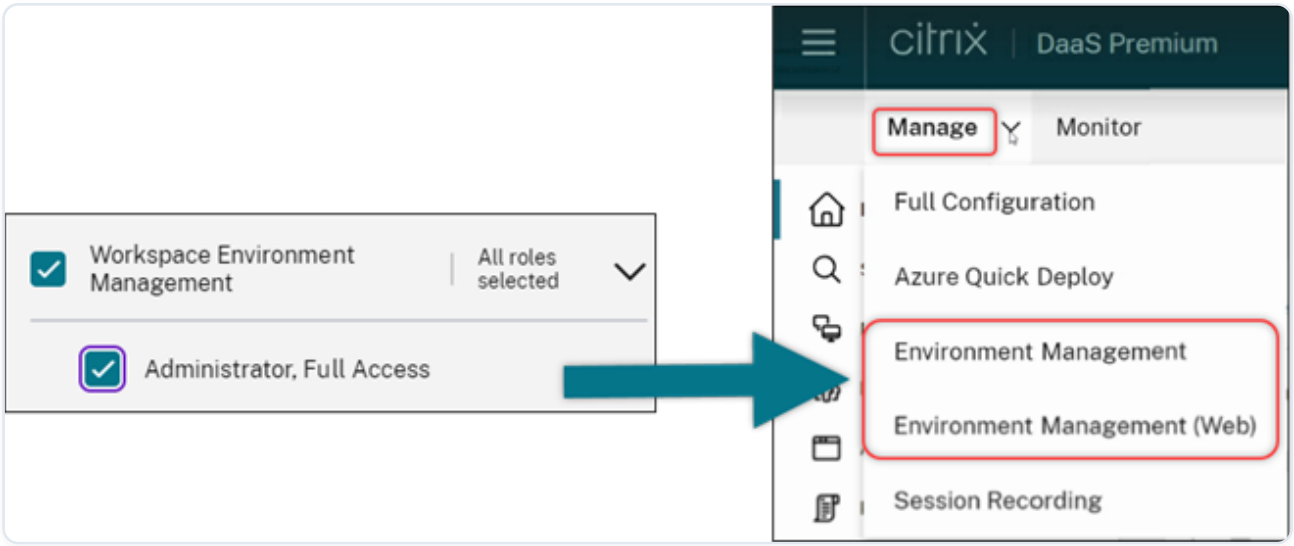
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Select the **StoreFront** node, click a server record, and then select **Configure Client Settings** in the action bar.
- Select the **Policies** node and then select **Configure Client Settings** in the action bar.

Support for managing user assignments for Citrix Cloud-managed delivery groups using Full Configuration. As part of our plan to migrate user assignment management from Cloud Library to Full Configuration, you can now manage user assignments for Citrix Cloud-managed delivery groups through Full Configuration. To accomplish this task, edit a target delivery group in **Full Configuration > Delivery Groups** and designate users permitted to use desktops or applications through one of these menus: **Desktops** (or **Desktop Assignment Rules**) or **Application Assignment Rule**. For more information, see Manage delivery groups.

Updates made in one portal seamlessly synchronize with the other, ensuring consistent updates across both portals.

Limit WEM console access to the WEM Full Access Administrator role. We've enabled access control for the Workspace Environment Management™ (WEM) consoles to prevent unauthorized entry. Only users with the **Workspace Environment Management Full Access Administrator** role can now use **DaaS > Manage** to access the WEM consoles.



Full Configuration: Azure catalogs support for inheriting DES settings from master images. Previously, Full Configuration set the Azure catalogs' default DES settings only based on machine profiles. We've now expanded this capability. With this enhancement, in the following cases, Full Configuration sets an Azure catalog's default DES settings directly based on the master image:

- If a machine profile isn't selected
- If the profile specifies a Platform Managed Key (PMK)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Create a machine catalog using an Azure Resource Manager image in the Full Configuration interface.

Enhanced search: More filters for enhanced precision. We've enhanced the search on the Search node to include two new filters, Zone and Provisioning Type, for enhanced precision and improved usability.

Full Configuration: Support for selecting Google Cloud machine type for GCP machine catalogs. With this feature, administrators have the flexibility to select the required memory and processor configurations for provisioned GCP VMs, tailoring them to meet specific operational requirements. For more information, see Create a machine catalog using the Full Configuration interface.

Support for global and regional customer-managed encryption keys (CMEK) for provisioning GCP VMs. You can now use global and regional CMEK keys for provisioning VMs from any provisioning project. This enhancement provides greater flexibility in key selection for provisioning VMs and improving VM security.

December 2023

New and enhanced features

Send Message progress. You can now view the progress of the **Send Message** operation available in **Monitor** > **Filters**. This operation helps send bulk messages to all connected sessions on your Site. The progress of the operation is displayed in percentage. Once the operation is completed, the system displays the number of messages that were sent and the number that have failed. Send message status is helpful when you are administering large sites. It helps understand if the message needs to be resent to certain users. Sending messages can fail if the machines are unregistered or if the sessions are faulty. For more information about Send Message, see Send messages to users.

Citrix Probe Agent authentication support via Citrix Gateway with domain credentials and Multi-factor authentication.

Citrix Probe Agent for application and desktop probing now supports authentication via Citrix Gateway with domain credentials and Multi-factor authentication. This feature helps to run the Probe Agent on machines that are connected to StoreFront via Citrix Gateway. The comprehensive probe results available on Monitor help troubleshoot issues related to the applications, hosting machine, or connection before the users experience them. Support for Citrix Gateway with Multi-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

factor authentication is available only for Citrix Gateway that is configured with LDAP and Native OTP using Single Login Schema. For more information, see Application and Desktop Probing

Redesigned Access Policy UI for more flexible resource access control. We've redesigned the **Edit Delivery group > Access Policy** UI to give you more flexibility in managing resource access for delivery groups. The following are the key features available with the new design:

- **Support for adding policies.** You can now add access policies to restrict resource access based on attributes of user connections. A policy can consist of two types of criteria:
  - **Inclusion criteria.** Let you specify user connections that are allowed to access the delivery group.
  - **Exclusion criteria.** Let you specify user connections that are prohibited from accessing the delivery group.
- **Expanded filter support.** You can now define inclusion and exclusion criteria using a range of SmartAccess filters. Those filters include Workspace filters such as `Citrix.Workspace.UsingDomain` and `Citrix-Via-Workspace`, as well as filters for network location-based adaptive access.
- **Match All logic support for included criteria.** The new logic enables you to achieve a high level of precision and control when specifying allowed user connections for delivery groups.

For more information, see Restrict access to resources in a delivery group.

November 2023

New and enhanced features

Support for creating Citrix Provisioning catalogs using Full Configuration interface. To create a Citrix Provisioning catalog, you had to use the Citrix Virtual Apps and Desktops Setup Wizard. With this feature, you can now create a Citrix Provisioning catalog using the Full Configuration interface and PowerShell.

This implementation provides you the following advantages:

- A single unified console to manage both MCS and Citrix Provisioning catalogs.
- Have new features for Citrix Provisioning catalogs, such as, identity management solution, on-demand provisioning and so on.

Currently, this feature is available only for Azure workloads. For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Introducing search for Application Groups. We have introduced the search functionality for application groups in the **Applications** node. With this enhancement, you can now directly search for an application group inside any application folder. For more information, see Search for Application Groups.

Modified configuration limits. The following table describes the modifications made to the DaaS configuration limits to improve the performance and provide cost-effectiveness.

RESOURCE	OLD LIMIT	NEW LIMIT
Active Directory domains	85	100
Catalogs	1000	2000
Delivery Groups	1000	2000
Resource location	85	100
Resource location -> Total sessions	20,000	25,000

For more information, see Limits.

A single option to retain VM and system disk during power cycles. Starting an existing VM on Azure is now faster than launching a new one, making it a more efficient choice to retain VMs across power cycles. In response to this change, we've combined the options **Retain VMs across power cycles** and **Retain system disk during power cycles** into a single option **Retain VM and system disk during power cycles**. This means that when you select this option to reduce VM restart times by retaining system disks, your VMs are retained as well.

New capability in Full Configuration to filter machine sizes based on *Encryption at Host property* in machine profiles (Azure VMs specific). Once you choose a machine profile with *Encryption at Host* enabled during Azure machine catalog creation or management, only machine sizes that support this feature are displayed.

Restrict backup and restore actions to Full Administrator role. We've enhanced access control for the backup and restore actions. Only users with the Full Administrator role can now access the **Backup + Restore** node, preventing unauthorized actions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data caching for the Search node. We have introduced data caching for the Citrix DaaS **Search** node. This enhancement improves the performance of the search and the following lists the use cases that ease your regular tasks:

- Quick display of search results after they are retrieved for the first time.
- Retains pagination results after navigating out and back to the **Search** node.

Image information on the Machine Catalogs page. You can now view the following image information through the **Template Properties** of the machine catalog:

- Operating system
- Machine identity service
- Machine Creation Service storage
- Filepath for `pagefile.sys` for Azure deployments.

This enhancement provides better clarity on the image information and ensures that the administrators have all the information about the machine catalog in one place.

Support for pinning search filters. To provide a quick search experience, Full Configuration enables a facility to pin your search filters. Filter pins allow you to keep the frequently used search filters accessible on the page. This enhancement is available in the search panels of the following nodes:

- **Search**
- **Machine Catalogs**
- **Delivery Groups**
- **Applications**

For more information, Use Search in the Full Configuration management interface.

Support for associating metadata with configuration logs. Using this enhancement, you can now attach metadata with the configuration logs by associating a `name-value` pair on the high-level operations. For more information, see Associate metadata with configuration logs.

Ignore orphaned resources with specific tag. In Azure environments, a customer-managed resource tagged with all Citrix tags is detected as an orphaned resource. With this feature, if you add another tag `CitrixDetectIgnore` with value as true to that resource, then the resource is ignored while detecting orphaned resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Solution for SCCM duplicated GUID issue. After creating multiple VMs using MCS, the System Center Configuration Manager (SCCM) displayed only one VM on its console because of duplicated GUIDs. This issue is now resolved by adding a step in the image preparation. This step deletes the existing certificates and GUID information within the master image. The step is enabled by default.

Repair the identity information of active computer accounts. With this feature, you can reset the identity information of active computer accounts that have identity-related problems. You can choose to reset only the machine password and trust keys, or reset all configuration of the identity disk. This implementation is applicable to both persistent and non-persistent machine catalogs. Currently, the feature is supported only for Azure and VMware virtualization environments. For more information, see Repair the identity information of active computer accounts.

Get encryption at host information associated with a machine profile. In Azure environments, with this feature, you can now know whether encryption at host is enabled for a machine profile input (VM or template spec) using PowerShell commands. For more information, see Retrieve encryption at host information from a machine profile.

Repair the user certificates of hybrid Azure AD joined machine identities. With this feature, you can use Powershell command to repair the user certificates of hybrid Azure AD joined machine identities if they corrupt or expire. For more information, see Identity pool of Hybrid Azure Active Directory joined machine identity.

Certificate expiry warning support for Hybrid Azure AD joined machine catalogs. Full Configuration now provides one-month advance warnings for user certificate expiration on Hybrid Azure AD joined machine catalogs. This enhancement aims to reduce the risk of service interruptions resulting from certificate expiration. To view the details and recommended actions, go to the **Machine Catalogs** node, select the machine catalog, and then click the **Troubleshoot** tab.

You can run the `Get-ProvScheme` command to get information about the user certificate expiration date of a hybrid Azure AD joined machine catalog.

Support for Azure confidential VMs (Preview). Azure confidential computing VMs ensure that your virtual desktop is encrypted in memory and protected in use. With this feature, you can now use MCS to create a catalog with Azure confidential VMs. You must use the machine profile workflow to create such a catalog. You can use both VM and ARM template spec as a machine profile input. For more information, see Azure confidential VMs (Preview).

Support for converting a non-machine profile-based machine catalog to machine profile-based machine catalog in AWS environment. In an AWS environment, you can now use a VM or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

launch template as a machine profile input to convert a non-machine profile-based machine catalog to machine profile-based machine catalog. New VMs added to the catalog take property values from the machine profile. For more information, see Convert a non-machine profile-based machine catalog to machine profile-based machine catalog.

Support for Citrix-managed HPE Moonshot plug-in (Preview). Previously, you used HPE-managed Moonshot plug-in (HPE Moonshot Machine Manager) maintained by Hewlett Packard Enterprise (HPE) to perform the power management actions on HPE Moonshot chassis. The plug-in was based on legacy APIs that made MCS infrastructure projects difficult. With this feature, a Citrix-managed HPE Moonshot plug-in (HPE Moonshot) is introduced. With this plug-in, you can create connections to your HPE Moonshot chassis, create catalogs, and power manage machines in the catalog using Full Configuration interface and PowerShell commands. For more information, see:

- HPE Moonshot virtualization environments (Preview)
- Connection to HPE Moonshot (Preview)
- Create an HPE Moonshot machine catalog (Preview)
- Manage an HPE Moonshot catalog (Preview)

Ability to change memory and disk cache size. With this feature, you can now change the memory and disk cache size of the Write-back cache (when MCSIO is enabled) using a PowerShell command without creating a new machine catalog. This implementation helps you to have the optimized cache configuration that is suitable for your business needs. This feature is applicable to:

- GCP and Microsoft Azure environments, and
- a non-persistent catalog with MCSIO enabled

For more information, see Change cache configuration on an existing machine catalog.

Support for creating a customer-managed encryption key enabled catalog. In Azure environments, you can now create a Citrix Provisioning catalog enabled with customer-managed encryption key (CMEK) using the Full Configuration interface and PowerShell commands. For more information, see Create a customer-managed encryption key enabled catalog.

Ability to copy tags on all resources in Azure. With this feature, in Azure environment, you can now copy tags specified in a machine profile to all the resources such as, multiple NICs and disks (OS disk, Identity disk, and write-back cache disk) of a new VM or an existing VM in a machine catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The machine profile source can be a VM or an ARM template spec. For more information, see Copy tags on all resources.

Session state updated to disconnected after the machine is suspended. Previously, after you suspended a VM, the session was still shown as **Active**. With this enhancement, after you suspend a VM, the associated session's state is now shown as **Disconnected**.

Support for creating AWS VMs that support hibernation. You can now create machine catalogs that support VM hibernation in your AWS environments, enhancing the overall cost-effectiveness of your deployment. You can also edit a catalog to include hibernation-capable VMs if the associated machine profile supports this capability. For more information, see Power Manage AWS VMs.

Support for configuring load-balancing methods at the delivery group level (Preview). This feature allows you to choose the **Vertical Load Balancing** method at a delivery group level. With this feature, each machine is aligned to the maximum load index before the next machine is powered on. Autoscale and Vertical Load Balancing determine when the next machine is powered on. This feature achieves maximum utilization for each machine and cost savings in public clouds. This feature offers more flexibility in managing the load balancing strategies for machines.

You can configure a delivery group to either inherit the load balancing method from the site-level settings or override the site-level load balancing method and instead choose one of the vertical or horizontal load balancing methods. For more information, see Step 2. Load balancing.

Support for hibernation-capable VMs in Azure (Preview). In Azure environments, you can create an MCS machine catalog that supports hibernation. Using this feature, you can suspend a VM, and then reconnect to the previous state of the VM when a user signs in again. For more information, see Create hibernation-capable VMs (Preview).

DaaS get-started guide. We've launched a new guide to streamline and simplify DaaS deployment and configuration for both new and experienced administrators. It offers these key benefits:

- **Easy to get started.** Using a step-by-step questionnaire-based approach, this guide helps new administrators set up their deployments quickly. Contextual help info throughout the guide aids in understanding essential concepts and terminology.
- **Simplify complex configurations.** This guide includes pre-configured settings where applicable and provides access to the Full Configuration UI for advanced setup. Experienced admins can use it as a foundation for more complex configurations.

For more information, see Use DaaS get-started guide.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assign drive letters to write-back cache disks using Full Configuration. Previously, you could assign a specific drive letter to the write-back cache disk only by using a PowerShell cmdlet. You can now accomplish the same task using Full Configuration. For more information, see Create machine catalogs.

Support for changing various Azure machine properties using Full Configuration. For Machine Creation Services-provisioned Azure machines, you can now change the following property settings using Full Configuration:

- Storage type
- Dedicated host group
- Azure Compute Gallery settings

When you change any of these settings, Full Configuration automatically identifies related settings and provides automatic synchronization or prompt messages requesting you to reselect related settings. This capability ensures consistent changes across associated settings, preventing potential configuration errors. For more information, see Edit a catalog.

Use existing identity pools to create identities for MCS-provisioned machines. When creating AD-joined catalogs or adding machines to them using Full Configuration, you can now use an existing identity pool to allocate machine identities. This feature allows you to apply a consistent machine account naming scheme across multiple catalogs. For more information, see Machine identities.

Session Topology. The Session Topology view is the next step towards enhancing troubleshooting workflows in Monitor. The Session Topology view provides a visual representation of the in-session path for connected HDX sessions. You can access the topology view from the **User Details > Session Performance**.

The Session Topology view for an HDX connected session shows the components involved in the session path with their metadata, the link between the components, and the applications published on the VDA. In addition, ICA Latency and ICA RTT measurements are displayed for the session when it is in a connected state.

Use the Session Topology view to understand the components through which the session data flows and to identify the specific hop that might be bringing in performance issues. For more information see Session Topology.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

October 2023

New and enhanced features

Refine your Autoscale settings using historical usage. A new Autoscale settings tab called **Autoscale Insights**, offers a comprehensive graph that visually compares your Autoscale settings and machine usage data from the previous week. With this graph, you can gain insights into the effectiveness of Autoscale settings:

- **Not cost-effective**. Financial waste exists due to the over-provisioning of capacity.
- **Poor user experience**. User experience is negatively impacted due to the under-provisioning of capacity.
- **Good balance between user experience and cost**. The capacity provisioned is aligned with the historical usage.

For more information, see Analyze the effectiveness of Autoscale settings.

Multiple NICs support for Azure VMs. With Full Configuration, you can now create Azure VMs with multiple NICs. A VM's maximum NIC count is determined by the machine size setting while its actual NIC count allowed is defined by the machine profile setting. For more information, see Create machine catalogs.

For creating or updating a catalog with multiple NICs per VM using PowerShell commands, see Create or update a catalog with multiple NICs per VM.

Trends for Session Performance metrics. Monitor is introducing a new **User Details > Session Performance** tab with enhanced troubleshooting workflows starting with the ability to correlate real-time metrics in identifying issues within user sessions. Session Experience now contains trends of session metrics like ICARTT, ICA Latency, Frames Per Second, Output Bandwidth Available, and Output Bandwidth Consumed. This feature helps reduce the mean time for resolution by enabling you to correlate multiple performance metrics in a single view. For more information see the User Issues article.

Support VDA version on settings page of create/edit policy. As part of creating a policy, when configuring the settings, the system provides an option to view the settings type. You can view the following settings type:

- All settings - View all settings for all VDA versions
- Current settings only - View settings for only the current VDA versions
- Legacy settings only - View settings for only the deprecated VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Create policies

Limit application visibility only supported for Active Directory accounts. The capability to limit the application visibility is available only for the Active Directory user accounts, and not for Azure Active Directory and Okta accounts. Note that to aid this feature, on the application setting workflow, on the Select Users or Groups page, **Azure Active Directory**, and **Okta** options in the **Select Identity type** field are disabled.

New UI option to delete VM records only from the Citrix site database. When catalog and VM deletion fails due to an unreachable hypervisor, you can now opt to only delete VM records from the Citrix site database, leaving the VMs intact on the host. For more information, see Delete a catalog.

Support for creating empty machine catalogs for non-MCS-provisioned machines. Creating empty machine catalogs now extends to non-MCS-provisioned machines, including:

- Virtual or blade machines provisioned using technologies other than Machine Creation Services.
- Physical machines not power managed by Citrix DaaS
- Remote PC Access machines

With this feature, you can now create machine catalogs without the need to add machines to them during catalog creation.

Image Refresh enhancements. Previously, when refreshing images, all images in the image tree were updated, irrespective of whether a specific node in the tree was selected. With the latest enhancement, if you've selected a node, only images in this node are refreshed. This enhancement ensures a more targeted refresh process, significantly improving the image refresh speed. Additionally, you can now clear a selected node in the image tree by holding CTRL and clicking the node. For more information, see Master image.

Peak Autoscale Assigned PowerOn. When persistent desktops are powered on but remain unused or if no user logs on, the administrators can define the wait time to take actions like, no action, suspend, or shutdown.

For assigned machines, where it is powered on but a session has not been connected to it within the set time after the start of peak time, then you can add a policy to the delivery group level to turn off the machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For assigned machines, where it is in resumed state but a session has not been connected to it within the set time after the start of peak time, then you can add a policy to the delivery group level to suspend the machine.

This feature is helpful if there is an end user who is on PTO, or has not logged on, or if a company has a long weekend, then you can set the wait time and machine disconnection actions to take to help reduce the Azure consumption cost. For more information, see Single-session OS random delivery groups and Single-session OS static delivery groups.

Monitor multiple Citrix DaaS instances (Preview). You can now use Citrix Monitor to monitor and troubleshoot issues across multiple Citrix DaaS instances. Citrix DaaS allows customers to aggregate multiple service instances using a hub and spoke model. With this configuration, administrators can perform helpdesk search on all configured DaaS instances from a single Monitor console. For more information regarding the configuration required to aggregate the spoke service instances to a hub, see Aggregate multiple Citrix Virtual Apps and Desktops service instances. Monitor supports the aggregation of up to four DaaS tenants (spokes) under a single DaaS tenant (hub). To have unified monitoring across all DaaS tenants, use bi-directional enumeration of the hub and spoke instances. For more information, see Aggregated Search across multiple DaaS instances (Preview).

Support for vSAN 8.0. You can now use MCS to provision VMs in the vSAN 8.0 environment.

Preserve NIC settings on provisioned VMs. Previously, the NIC settings of the master image were not retained in the provisioned VMs. For example, if you configured the DNS settings on the master image, the provisioned VMs did not retain the configured DNS settings of the master image. With this feature, the provisioned VMs can now retain the NIC settings of the master image. The settings are retained even after a Windows update. The filter driver is automatically installed if you do a fresh installation of VDA version 2308 or later on a Hyper-V deployed machine through the MCS master image installations. However, currently, if you upgrade from an older version of VDA (version less than 2308) and want to install the filter driver, then you must select the checkbox **Citrix HyperV Filter Driver** on the **Additional Components** page while upgrading the VDA. For more information, see Install additional components.

This feature is applicable to:

- Hyper-V VMs (including Azure and SCVMM)
- Persistent and non-persistent MCS machine catalogs
- Non-persistent MCS machine catalogs with MCSIO
- Master image with multiple NICs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Detect Orphaned Azure resources. With this feature, you can now detect the orphaned resources in your Azure deployment, enabling efficient resource management. After the orphaned resources are identified, you can take further action, bringing in more productivity and cost reduction. For more information, see Detect Orphaned Azure resources in your deployment.

New image update status. When monitoring image update statuses for catalogs in Full Configuration, you can now view a new status **Preparing image**, in addition to the existing ones **Fully updated**, **Partially updated**, and **Pending update**. For more information, see Change the master image.

PowerShell commands to create Auto-tags (Preview). With this feature you can now create tags automatically by using the PowerShell command. For more information, see Auto Tags.

Notification sign is shown to user or delivery group. While creating or modifying a policy and configuring the settings, if all delivery groups are disabled, the system displays a warning that - None of the elements in this filter is enabled. If at least one delivery group is enabled, the system does not display the warning sign. For more information, see Policy settings

September 2023

New and enhanced features

PowerShell commands to manage Local Host Cache (LHC). You can now use PowerShell commands to manage LHC on Citrix Cloud Connectors. For more information, see Local Host Cache PowerShell commands.

Support for creating empty machine catalogs. In Full Configuration, you can now create a machine catalog without immediate VM creation. With this feature, you can postpone VM creation until back-end hosts are fully prepared or VM provisioning is completed, gaining more flexibility in creating catalogs. Currently, this feature applies only to Machine Creation Services-provisioned catalogs. For more information, see Create machine catalogs.

Data caching for the Home node. We've introduced data caching for the Citrix DaaS **Home** node. This enhancement improves the user experience by reducing the page load times when you navigate to the **Home** node.

Search enhancements for applications. We've revamped the search functionality in the **Applications** node to align with the new design introduced in the **Search** node. This new feature improves your application search experience and maintains a consistent search experience across DaaS. The keyword **Application Name** in the filter expression is renamed to **Name**, while retaining

© 1997–2026 Citrix Systems, Inc. All rights reserved.

its original meaning. For more information, see Use Search in the Full Configuration management interface.

Enhanced scope management: showing objects in folder view. On the scope creation and management pages, machine catalogs, delivery groups, and application groups are now displayed in folder structures that align with their management in DaaS. This folder view simplifies the process of selecting objects for scope creation and management, making your choices more intuitive and straightforward. For more information, see Create and manage scopes.

Removed the Leave user management to Citrix Cloud option. When creating a delivery group in Manage > Full Configuration, on the Users page, the support for this option is removed. For delivery groups where user assignments were handled through Citrix Cloud, continue to manage user assignments within the Citrix Cloud library.

Removed the Azure Germany option. In line with the closure of Microsoft Cloud Deutschland on October 29, 2021, we've removed the **Azure Germany** option from the host connection creation page.

Proactive service alerts in Full Configuration. Alerts come at two levels — site-wide alerts shown in Home (flag icon) and zone-related alerts shown on the Troubleshoot tab of each zone. Currently, this feature gives you proactive warnings and alerts to make sure that your Local Host Cache and zones are configured correctly so that when an outage occurs, Local Host Cache works and your users are not impacted. For more information, see Service health alerts and Zones.

August 2023

New and enhanced features

Full Configuration: Support for provisioning AWS and GCP VMs using machine profiles. When provisioning AWS or GCP VMs using Machine Creation Services (MCS), you can now select an existing VM as the machine profile, letting VMs within the catalog inherit settings from the selected VM.

- For GCP VMs, the inherited settings include Disk Encryption Set ID, Machine size, Storage type, and Zone.
- For AWS VMs, the inherited settings vary based on the stage:
  - During catalog creation: Machine size, Tenancy type, Security group, and the number of NICs.
  - During catalog editing: Machine size and Security group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Create a machine catalog.

Introducing search functionality in Machine Catalogs and Delivery Groups nodes. You can now directly search and locate machine catalogs and delivery groups within the **Machine Catalogs** and **Delivery Groups** nodes. The search functionality in these nodes provides the same interface as the **Search** node, providing seamless search experience across DaaS. For more information, see Use Search in the Full Configuration management interface.

View endpoint device status in Session Launch Diagnostics using Device Posture. The Session Launch Diagnostics feature in Monitor helps narrow down to the exact component and stage where a session failure occurred. This helps identify the exact reason for a session launch failure and take the recommended action.

As the next step in making this check comprehensive across all the components involved in the session launch sequence, you can now view the endpoint device scan results. Clicking **Endpoint Device** in the list of components shows the Device Posture scan status. Device Posture Service scans the endpoint device for compliance based on policies defined by the administrator.

Ensure that the Device Posture service is configured with DaaS as described in the Device Posture article. Errors logged by Device Posture are described in Device Posture Error Logs.

For more information, see Steps to diagnose session launch failure

New options in Full Configuration to route API requests to Azure and GCP through Citrix Cloud Connectors. Previously, API requests to Azure and GCP could be routed only through public endpoints. With a new option in **Full Configuration > Add Connection and Resources**, you can now opt for a more secure approach by routing them through Citrix Cloud Connectors. For more information, see Create a service principal and connection using Full Configuration.

Search and filter enhancements. We've made the following enhancements to improve your search experience:

- **Simplified search**: Performing a search without filters now removes search recommendations, providing a clean and straightforward search experience.
- **AND/OR operator update**: "Match all(AND operator)" and "Match any(OR operator)" options are now available in the filters panel, accessible with a single click the filters icon.
- **Streamlined filter configuration**: You can now specify and apply multiple filters seamlessly with the filters panel.
- **Cleaner interface**: The "filter pinning" ability has been removed, reducing UI clutter and making your search experience more intuitive.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Quick filter addition**: After applying filters, you can now use the plus sign to quickly add one more filter.
- **Delete saved filter sets**: You can now easily delete saved filter sets right within the search menu, without navigating to **Manage filter sets**.

For more information, see Use Search in the Full Configuration management interface.

VDA upgrade support for Azure Quick Deploy-created machine catalogs. With Full Configuration, you can now enable **VDA Upgrade** for machine catalogs created through Azure Quick Deploy and then perform **Upgrade VDA** on them for immediate or scheduled upgrades. For more information, see Upgrade VDAs using the Full Configuration interface.

Ability to reset the OS disk of a persistent VM in an MCS created machine catalog in SCVMM. You can now use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. The feature automates the process of resetting the OS disk. For example, it helps in resetting the VM to its initial status of a persistent development desktop catalog created using MCS. Currently, this feature is applicable to Azure, Citrix Hypervisor, SCVMM, and VMware virtualization environments. For more information on using the PowerShell command to reset the OS disk, see Reset OS disk.

Update properties of individual VMs. You can now update properties of individual VMs in a persistent MCS machine catalog using a PowerShell command. This implementation helps you to manage individual VMs efficiently without updating the entire machine catalog. Currently, this feature is applicable only to the Azure environment. For more information, see Update properties of individual VMs.

Restrict upload and download of managed disks. As per Azure policy, you cannot upload or download more than five disks or snapshots at the same time with the same disk access object. With this feature, the limit of five concurrent uploads or downloads is not enforced if you:

- Configure `ProxyHypervisorTrafficThroughConnector` in `CustomProperties`, and
- Do not configure Azure policy to create Disk Accesses automatically for each new disk to use private endpoints.

Support for assigning a specific drive letter to MCS I/O write-back cache disk. Previously, the Windows operating system automatically assigned a drive letter to MCS I/O write-back cache disk. With this feature, you can now assign a specific drive letter to an MCS I/O write-back cache disk. This implementation helps you to avoid conflicts between the drive letter of any applications that you use and the drive letter of MCS I/O write-back cache disk. This feature is applicable to only

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows operating system. For more information, see Assign a specific drive letter to MCS I/O write-back cache disk.

Support for machine profile in Citrix Hypervisor. In Citrix Hypervisor, you can now create an MCS machine catalog using a machine profile. The source of the machine profile input is a VM. The machine profile captures the hardware properties from a VM template and applies them to the newly provisioned VMs in the catalog. For more information, see Create a machine catalog using a machine profile.

Retry creating catalog after failure. When catalog creation fails, you can now retry creating the catalog. To ensure successful creation, check the troubleshooting information and resolve the issues. The information describes the issues found and provides recommendations for resolving them. Failed catalogs are marked with an error icon. To see the details, go to the **Troubleshoot** tab of each catalog. For more information, see Manage machine catalogs.

Permission for managing configuration sets. To enable more precise control over WEM configuration set management, we've introduced a new permission called **Manage configuration sets** to the **Machine catalogs** permission set. This permission grants exclusive access to users who can perform tasks such as binding or unbinding a configuration set and switching to a different configuration set for catalogs. For more information, see Manage configuration set for a catalog.

New option in Full Configuration to enable cleanup of stale Azure AD joined devices. We've introduced an option in Full Configuration to simplify the cleanup of stale Azure AD joined devices in Citrix DaaS. Previously, you had to run a custom PowerShell script to perform the task. Enabling this option grants host connections permission to automatically clean stale Azure AD joined devices. For more information, see Azure host connections.

Monitor image update status for catalogs using Full Configuration. You can now monitor image update statuses for non-persistent machine catalogs using a new column, **Image Update**. This column indicates whether images of a catalog are **Fully updated**, **Partially updated**, or **Pending update**.

To show the column in the **Machine Catalogs** table, follow these steps:

1. In the **Machine Catalogs** node, select the **Columns to Display** icon in the action bar.
2. Select **Machine Catalog > Image Status**.
3. Click **Save**.

Displaying the **Image update** column might degrade the console performance. We recommend displaying it only when necessary.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure environment for GCP-managed traffic. With this feature, you can now allow only private Google access to your Google Cloud projects. This implementation enhances security to handle sensitive data. To do this, add `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` in case of Citrix Cloud deployment. If you are using a private worker pool, add `UsePrivateWorkerPool` in `CustomProperties`. For more information, see Create a secure environment for GCP managed traffic.

July 2023

New and enhanced features

Support for getting a list of orphaned resources on Azure. In Azure environments, you can now get a list of orphaned resources that are created by MCS but are no longer used by MCS. This feature helps to avoid extra costs. For more information, see Retrieve a list of orphaned resources.

Support for creating persistent multi-session machines using Full Configuration. When creating a catalog of multi-session machines, you can now specify whether to make them persistent. For persistent multi-session machines, keep in mind that changes users make to the desktops are saved and accessible to all authorized users. For more information, see Create machine catalogs.

New capability in Full Configuration to filter the AWS AMI inventory. When selecting machine templates during AWS catalog creation, you can now filter the AWS AMI inventory for a target template using these search criteria:

- Image name
- Image ID
- Image tags

The machine template list loads dynamically as you scroll down the list - 25 items are initially loaded and more loaded as you scroll.

Support for deleting Azure AD devices. With this feature, stale Azure AD devices can be consistently deleted by assigning the Cloud Device Administrator role to the service principal and modifying the custom property of the hosting connection. If you do not delete the Azure stale AD devices, then the corresponding non-persistent VM stays in the initializing state until you manually remove it from the Azure AD portal. For more information, see Identity pool of Azure Active Directory joined machine identity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for machine profile in AWS environment. When you create a catalog to provision machines using Machine Creation Services (MCS) in AWS, you can now use a machine profile to capture the hardware properties from an EC2 instance (VM) or launch template version and apply them to the provisioned machines. Properties that are captured can include, for example, EBS volume properties, instance type, EBS optimization, and other supported AWS configurations. When editing the catalog, the machine profile of the provisioned machines can be changed by providing a different VM or launch template. For more information, see Create a catalog using a machine profile.

Export limit on search results extended to 30,000 from 10,000. We've extended the export limit on search results. Previously restricted to 10,000 items, you can now export up to 30,000 items to a CSV file. For more information, see Export search results to a CSV file.

Image refresh option. When selecting master images for machine catalogs, you can now quickly get the most up-to-date master image list using the **Refresh** option at the top right. Note that the **Refresh** option is not available for AWS catalogs. Additionally, a **Refresh** option is available for machine profiles and host groups in Azure catalogs.

June 2023

New and enhanced features

Support for getting custom properties from the machine profile input in GCP. Previously, in GCP environments, while creating an MCS machine catalog using a machine profile input, you had to explicitly specify the custom properties. The action forced an extra effort. With this feature, you can now derive the following custom properties without explicitly defining them:

- `ServiceOffering`
- `CryptoKeyId`
- `CatalogZones`
- `Storage`

When you run `New-ProvScheme` and `Set-ProvScheme` commands and do not explicitly specify the custom properties, then the values of the properties are derived from the machine profile input.

For example, `New-ProvScheme -MachineProfile` writes the machine profile's machine type to the provisioning scheme's `ServiceOffering` property unless you specify `ServiceOffering` in the `New-ProvScheme` command. If you run `Set-ProvVMScheme` twice, then the most recent command takes effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remove tags in AWS environments. Previously, `Remove-ProvVM` and `Remove-ProvScheme` PowerShell commands with `ForgetVM` parameter removed the VMs and machine catalogs from the Citrix database. However, the commands didn't remove the tags. You had to individually manage the VMs and machine catalogs that weren't removed entirely from all the resources. With this feature, you can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and tags from a single VM or a list of VMs from a machine catalog.
- `Remove-ProvScheme` with `ForgetVM` parameter to remove a machine catalog from the Citrix database and resources from a machine catalog.

This implementation helps in:

- Identifying leaked resources
- Removing the additional cost of maintaining the resources that are not required

This feature is only applicable to persistent VMs. For more information, see Remove tags.

Ability to get historical errors and warnings associated with an MCS machine catalog. Previously, you only got the latest warnings and errors associated with a machine catalog. With this feature, you can now get a list of the historical warnings and errors of an MCS machine catalog. This list helps you to understand any issues with your MCS machine catalog and fix those issues.

For more information, see Retrieve warnings and errors associated with a catalog.

Increased capacity with improved performance for Citrix in Google Cloud. Citrix can now support catalogs containing up to 3,000 VDAs in a single Google Cloud project. This update brings performance improvements to both provisioning and power management operations.

Ability to reset the OS disk of a persistent VM in an MCS created machine catalog in Google Cloud and AWS environment. You can now use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. The feature automates the process of resetting the OS disk. For example, it helps in resetting the VM to its initial status of a persistent development desktop catalog created using MCS. Currently, this feature is applicable to AWS, Azure, Citrix Hypervisor, Google Cloud, and VMware virtualization environments. For more information on using the PowerShell command to reset the OS disk, see Reset OS disk.

Support for changing disk related custom properties of an existing catalog and existing VMs in GCP. Previously, in GCP environments, you could add the custom properties only when

© 1997–2026 Citrix Systems, Inc. All rights reserved.

you created the MCS machine catalog. With this feature, you can now change the following disk-related custom properties of an existing catalog and existing VMs of the catalog.

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

This implementation helps you to select different storage types for different disks even after you create a catalog and thus, balance pricing associated with different storage types. For more information, see Change disk related custom properties of an existing catalog.

Dynamic session timeout support extended to VDA version 2203 LTSR CU3 or later. For single-session OS delivery groups, this feature now applies to VDAs of version 2206 CR or later, or 2203 LTSR CU3 or later. For more information, see Dynamic session timeouts.

Improved host connection creation experience in Full Configuration. After you select a resource location, the **Connection type** drop-down list now displays all Citrix-supported hypervisors and cloud services, and their availabilities depend on:

- For a resource location without accessible Cloud Connectors, only hypervisors and cloud services that support connectorless deployments are available.
- For a resource location with accessible Cloud Connectors, only hypervisors and cloud services that have their plug-ins properly installed on those connectors are available.

For more information, see Create and manage connections.

Additional component selection in VDA upgrade. You can now select which additional components to upgrade or install while upgrading a VDA. For more information, see upgrade VDAs.

IMPORTANT:

To use the additional components feature, make sure that your VDA Upgrade Agent is version 7.34 or later, which is included in the VDA installer version 2206 or later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Full Configuration now preconfigures certain settings for Azure machines based on machine profiles. When you provision Azure VMs, Full Configuration now preconfigures the following settings based on the selected machine profile:

- Host group
- Disk Encryption Set
- Availability Zone
- License Type

Support for AWS instance hibernation. You can now launch AWS instances, set them as desired, and hibernate them. The hibernation process stores the in-memory state of the instance, along with its private and elastic IP addresses, allowing it to pick up exactly where it left off. For more information on creating VMs that support hibernation, see Instance Hibernation.

Support for optimizing AWS throttling. You can now power on and off a large number of machines in an AWS catalog without encountering throttling issues. Throttling issues occur when the number of requests sent to AWS exceeds the number of requests that the server can handle. This feature increases efficiency by reducing the number of AWS calls to power machines on and off in bulk. It also significantly reduces the time taken to power on and off machines in persistent catalogs.

Secure environment for Azure managed traffic. Previously, you relied on the public internet to let your Azure endpoints interact with resources in your environment. As a result, security concerns were raised because the public internet was accessed. With this feature, MCS enables network traffic to be routed through Citrix Cloud Connectors in your environment. This makes the environment safe because now all Azure managed traffic originates from your own environment. To do this, add `ProxyHypervisorTrafficThroughConnector` in `CustomProperties`. For more information, see Create a secure environment for Azure managed traffic.

After you set the custom properties, you can configure Azure policies to have private disk access to Azure managed disks.

Support for provisioning catalog VMs with Azure Monitor Agent. Azure Monitor Agent (AMA) collects monitoring data and delivers it to Azure Monitor. With this feature, you can provision MCS machine catalog VMs (persistent and non-persistent) with AMA installed as an extension. This implementation enables monitoring by uniquely identifying the VMs in monitoring data. For more information on AMA, see Azure Monitor Agent overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Currently, MCS supports only the machine profile workflow for this feature. For more information on provisioning machine catalog VMs with AMA enabled, see Provision catalog VMs with Azure Monitor Agent installed.

Enable restart schedule for an MCS catalog. Previously, you could schedule image updates by waiting for the next restart or by triggering an immediate restart of all VMs. With this feature, you can now create a one-time restart schedule for a catalog to be triggered on a desired date and time to facilitate MCS image updates. To create a restart schedule, use the `BrokerCatalogRebootSchedule` command. For more information, see Change the master image.

Manage expired client secrets in Azure Quick Deploy. In Azure Quick Deploy, you can now stay informed with alerts when client secrets expire, and easily update them to ensure continuous access to Azure resources. For more information, see Update expired client secrets.

May 2023

New and enhanced features

Search enhancements. This feature enhances visuals and interactions for filters, bringing you a better search experience. For more information, see Use Search in the Full Configuration management interface.

New user exclusions policy where you can define directory paths that are not redirected to the user layer. User exclusions apply to the user personalization layer (UPL), but not to the session host. Logoff.txt now contains all active user exclusions. For more information, see User personalization layer.

Support for updating hardware version of new VMs added in an MCS machine catalog. In VMware environments, you can now update the hardware version of the newly added VMs in an existing MCS machine catalog using a machine profile source. You do not have to create a new machine catalog to update the hardware version of the VMs added to a catalog. You must use the machine profile workflow to use this feature.

Support for filtering AWS VM instances. Previously, when you used an AWS VM instance as a machine profile input to create an MCS machine catalog, the catalog sometimes did not create or function correctly because of invalid machine profile input. With this feature, you can now list the AWS VM instances that can be used as valid machine profile VMs. To do this, use the `Get-HypInventoryItem` command. For more information, see Filtering VM instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for converting a non-machine profile-based machine catalog to machine profile-based machine catalog in Azure environment. In the Azure environment, you can now use a VM or template spec as a machine profile input to convert a non-machine profile-based machine catalog to machine profile-based machine catalog. Existing VMs and new VMs added to the catalog take property values from the machine profile unless overwritten by explicit custom properties. For more information, see Convert a non-machine profile-based machine catalog to machine profile-based machine catalog.

Support for double encryption on managed disk in Azure environment. In Azure environment, you can now create an MCS machine catalog with double encryption. Double encryption is platform-side encryption (default) and customer-managed encryption (CMEK). Therefore, if you are a high security sensitive customer who is concerned about the risk associated with any encryption algorithm, implementation, or a compromised key, you can opt for this double encryption. Persistent OS and data disks, snapshots, and images are all encrypted at rest with double encryption. For more information, see Double encryption on managed disk.

Support for machine profile in VMware. In VMware environments, you can now create an MCS machine catalog using a machine profile. The source of the machine profile input is a VMware template. The machine profile captures the hardware properties from a VMware template and applies them to the newly provisioned VMs in the catalog. For more information, see Create a machine catalog using a machine profile.

Ability to reset the OS disk of a persistent VM in an MCS created machine catalog in Azure and Citrix Hypervisor. You can now use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. The feature automates the process of resetting the OS disk. For example, it helps in resetting the VM to its initial status of a persistent development desktop catalog created using MCS. Currently, this feature is applicable to Azure, Citrix Hypervisor, and VMware virtualization environments. For more information on using the PowerShell command to reset the OS disk, see Reset OS disk.

Improved host connection creation experience. You can now get the following information while you create a host connection:

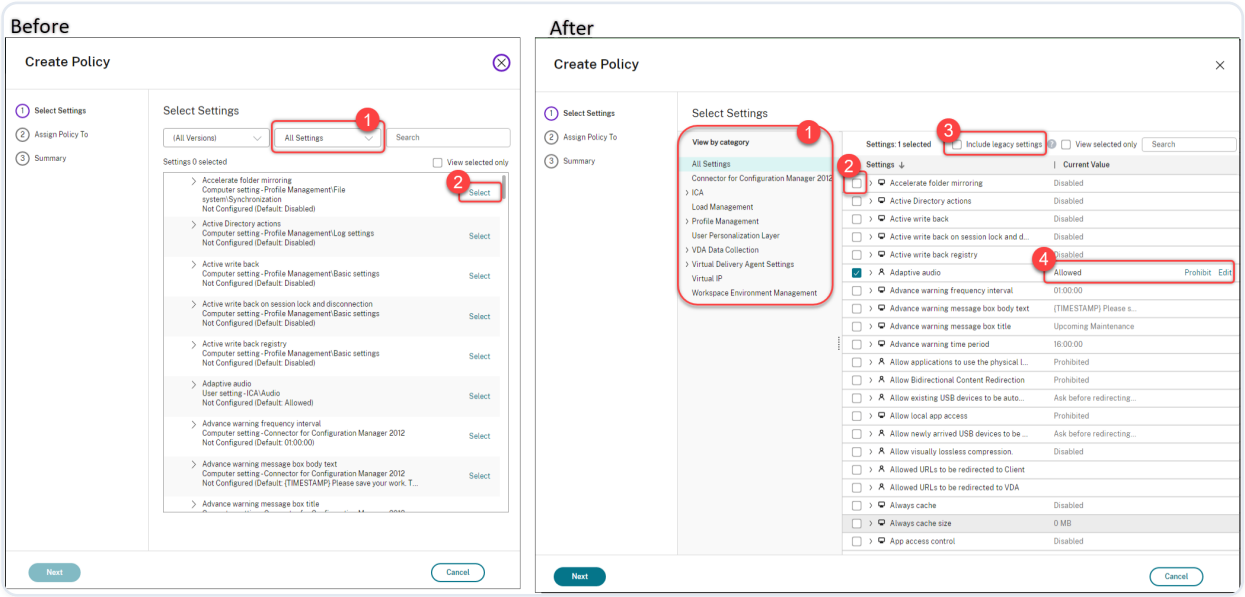
- List of all Citrix supported hypervisor plug-ins, including third party plugins
- Availability of hypervisor plug-in. If the availability status is false, possible reason might be that Cloud Connector is not installed

This feature helps you to correctly set-up a resource location and thus, create a host connection. For more information, see Step 1. Connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

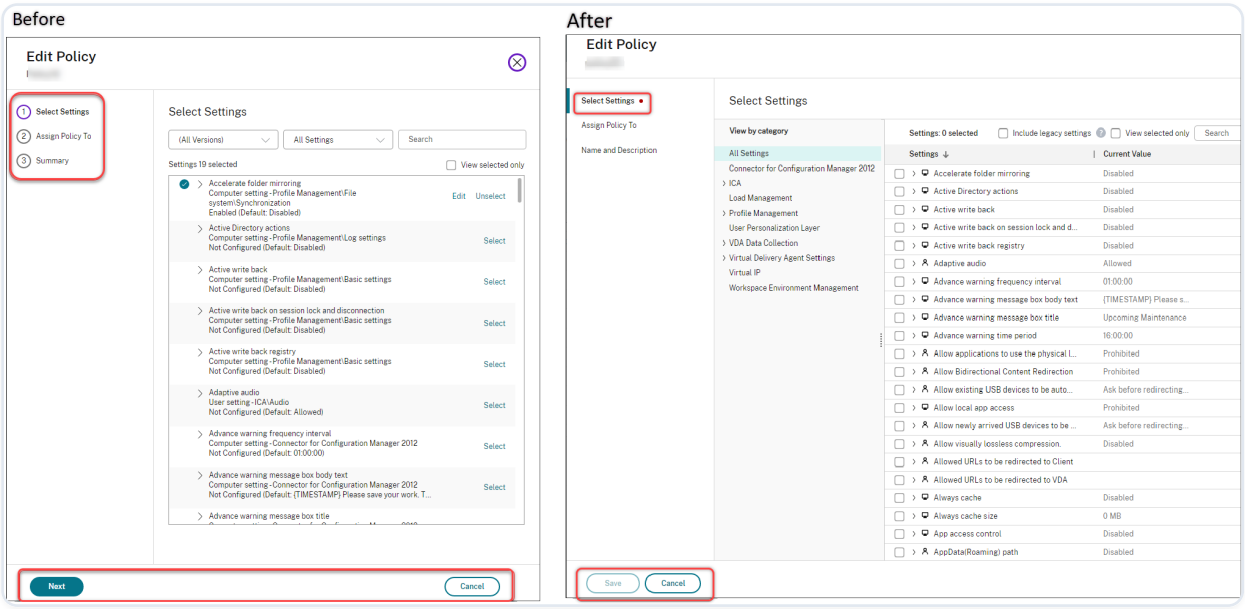
User experience improvements for the Policies node. To improve the user experience and make policy management more efficient, we've implemented the following improvements to the **Full Configuration > Policies** node:

- New UI design for the **Create Policy** and **Create Template** actions:
  - Expandable folder view for policy settings. On the **Select Settings** page, all settings are displayed by category in an expandable tree view, making it easier to find a setting.
  - To select a setting, you simply click a check box instead of using the **Select** button.
  - Legacy settings have been hidden by default so that only the most relevant settings are shown. If legacy settings are needed, select **Include legacy settings**.
  - An action button has been added next to a Boolean setting, enabling you to change its value directly in the settings list.



- New UI design for the **Edit Policy** action:
  - The navigation menu has been updated to an unordered list. Each item in the list now includes a **Save** button on its page. With this new design, you can save changes made to an item without having to navigate through all items in the navigation menu. These improvements make policy management more efficient and streamlined.
  - Red dots appear next to the navigation items to indicate setting errors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Drag to reprioritize policies. In the priority list, you can now change the priority of a policy by dragging it to a desired position.

New option to turn off forced user logoff for AutoScale. A new option, **Neither notify nor force user logoff**, is now available on the **Manage Autoscale > User Logoff Notification** page. With the option selected, Autoscale will neither force users to log off from machines in drain state nor notify users to log off and log on to a different machine. For more information, see User logoff notifications.

Ability to restart Windows 365 Cloud PCs. You can now use Citrix DaaS to restart Windows 365 Cloud PCs.

More session details. When you view a session in **Full Configuration > Search > Sessions**, the session view (in the lower pane) now includes more session details to help you troubleshoot and identify client issues:

- **Reconnect time.** The time when a session reconnected after being disconnected.
- **Client platform.** The platform used to launch the session.
- **Client version.** The version of the client platform used to launch the session.
- **Remote host IP.** The IP address of the remote host where Citrix Workspace is being hosted.

Support for renaming Azure AD security groups for VMs. For VMs added to an Azure AD security group through Citrix DaaS, you can now rename the security group using **Full Configuration > Edit Machine Catalog**. Renaming occurs after you save the change.

Default domain selection for machine accounts. When you create a catalog, the domain where the resource (connection) resides is selected by default for machine accounts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ability to display the Azure AD assigned security groups for VMs to join. In Full Configuration, when you create Azure Active Directory joined VMs, an option, **Join an assigned security group as a member**, is now available, letting you add the Azure AD security group where the VMs reside to an assigned security group. For more information, see Create a machine catalog using an Azure Resource Manager image.

Support for changing networks for connections. In Full Configuration, you can now change networks for a connection. You can't unassociate networks from a connection if they are in use. For more information, see Edit network.

Ability to remove tags in Azure environments. Previously, `Remove-ProvVM` and `Remove-ProvScheme` PowerShell commands with `ForgetVM` parameter removed the VMs and machine catalogs from the Citrix database. However, the commands didn't remove the tags from the resources. You had to individually manage the VMs and machine catalogs that weren't deleted entirely from all the resources. With this feature, you can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and tags created on the resources from a single VM or a list of VMs from a machine catalog.
- `Remove-ProvScheme` with `ForgetVM` parameter to remove a machine catalog from the Citrix database and tags created on the resources from an entire machine catalog.

This implementation helps in identifying orphaned resources that are created by MCS but no longer used by MCS.

This feature is only applicable to persistent VMs. For more information, see Remove tags.

Failed Machines alert.The Proactive Notification and Alerting feature of the Monitor is enhanced to include a new alert, Failed Machines (in %) based on the percentage of failed machines in a delivery group. The new alert condition, allows you to configure alert thresholds as a percentage of failed machines in a delivery group. For more information, see Failed Machines section in the Alerts article.

April 2023

New and enhanced features

Publishing with specific cloud platforms using Citrix Provisioning in Image Portability Service. Specific workflows for using Image Portability Service to publish in AWS, Azure, and Google Cloud are now available. In addition, the required permissions for Azure and networking have been updated. For more details, see Migrate workloads to public cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for identifying why a machine is in maintenance mode. Previously, PowerShell was your only choice to identify why a machine was in maintenance mode. You can now achieve that in Full Configuration:

1. Use Search to locate the machine.
2. Check **Maintenance Reason** on the **Details** tab in the lower pane. Or hover over the **Maintenance Mode** column. The following information can appear:

- By Administrator: Put into maintenance mode by administrator.
- Maximum Failed Registrations: Put into maintenance mode as machine exceeded maximum allowed registration attempts.

Also, a filter, **Maintenance Reason**, is now available. You can use it to identify the target machines.

The feature is useful for administrators to troubleshoot issues with machines in maintenance mode.

Use variables to notify users of remaining time before they are logged off. When forcing user logoff, you can now use `%s%` or `%m%` as variables to indicate the specified time in the notification message. To express the time in seconds, use `%s%`. To express the time in minutes, use `%m%`. For more information, see User logoff notifications.

Support for customizing power on behavior at storage type change failure. At power-on, the storage type of a managed disk might fail to change to the desired type due to a failure on Azure. Previously, in these scenarios, the VM would remain off with a failure message sent to you. With this feature, you can either choose to power on the VM even when storage cannot be restored to its configured type or choose to keep the VM powered off. For more information, see Customize power on behavior at storage type change failure.

Support for MAK activation. You can now provision persistent and non-persistent machine catalogs with VMs activated through the Multiple Activation Key (MAK). With this feature, now MCS can also communicate with provisioned VMs. This implementation helps in activating the Windows system without losing activation counts. For more information, see Volume licensing activation.

Support for Azure disk encryption at host. With this feature, you can now create an MCS machine catalog with encryption at host capability. Currently, MCS supports only the machine profile workflow for this feature. You can use a VM or a template spec as an input for a machine profile. For more information, see Azure disk encryption at host.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this type of encryption, the server hosting the VM encrypts the data and then the encrypted data flows through the Azure storage server. Therefore, this method of encryption encrypts data end to end. For more information, see Encryption at host - End-to-end encryption for your VM data.

Support for GCP instance template as an input for machine profile. With this feature, you can now select a GCP instance template as an input for the machine profile. Instance templates are lightweight resources in GCP, therefore are very cost effective. To do this, use PowerShell commands. For more information on using PowerShell commands to create and update machine catalogs by selecting a GCP instance template, see Create a machine catalog with machine profile as an instance template.

Support for modifying Azure AD dynamic security group name. You can modify or delete an Azure AD dynamic security group name from Azure portal. This action can make the Azure AD dynamic security group name out-of-sync with the dynamic security group associated with a machine catalog. With this feature, you can now modify the Azure AD dynamic security group name associated with a machine catalog.

This modification helps you to make the Azure AD dynamic security group information stored in Azure AD identity pool object to be consistent with the information stored in Azure portal. For more information, see Modify Azure AD dynamic security group name.

Added permissions required in GCP. The permissions required to do the following are now added:

- Create host connection
- Do power management of VMs
- Provision catalogs

For more information, see About GCP permissions.

Credential handling. For enhanced security, by default, credentials are not forwarded to the cloud for users who are not in the same domain as their VDAs. Login attempts fail when all of the following conditions are met:

- The user is in a domain different from the VDA
- No trust exists between the domains
- StoreFront is installed in the same domain as the VDA

Previously under these conditions, the user couldn't be authenticated to StoreFront. So, the Cloud Connector forwarded user credentials to the cloud to route the authentication request to the correct

© 1997–2026 Citrix Systems, Inc. All rights reserved.

destination for that user. This behavior can still be configured if needed. For more information, see the `CredentialForwardingToCloudAllowed` parameter of Set-Brokersite in the DaaS PowerShell SDK.

March 2023

New and enhanced features

Support for configuring role and scope for administrators. Citrix Cloud now supports a higher degree of flexibility and customization when configuring access for an administrator. Previously, you could only select predefined pairs of roles and scopes. With this enhancement, you can select a role and then pair it with the scope of your choice.

For more information, see Configure custom access for an administrator.

Support for creating dynamic security group under existing assigned security group. Previously, you could create Azure AD dynamic security groups for a machine catalog. With this feature, you can also add an Azure AD dynamic security group under an existing Azure AD assigned security group. You can do the following:

- Get security group information.
- Get all Azure AD assigned security groups that are synced from on-premises AD server or the assigned security groups to which Azure AD roles can be assigned.
- Get all Azure AD dynamic security groups.
- Add Azure AD dynamic security group as a member of Azure AD assigned group.
- Remove the membership between Azure AD dynamic security group and Azure AD assigned security group when Azure AD dynamic security group is deleted along with the machine catalog.

For more information, see Create an Azure AD dynamic security group under an existing Azure AD assigned security group.

Support for Azure AD dynamic security group for Azure AD joined VM. Citrix now supports dynamic security group for a catalog while creating an MCS machine catalog. Dynamic security group rules place the VMs in the catalog to a dynamic security group based on the naming scheme of the machine catalog. This is useful when you want to manage the VMs by Azure Active Directory (Azure AD). This is also useful when you want to apply Conditional Access policies or distribute apps from Intune by filtering the VMs with Azure AD dynamic security group. When you delete a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

catalog, the dynamic security group is also deleted. For more information, see Azure Active Directory dynamic security group.

For more information on license requirement for using dynamic security groups, see the Microsoft document Create or update a dynamic group in Azure Active Directory.

Support for adding VMs to Azure AD security groups through Full Configuration. An option, **Azure AD security group**, is now available when you create Azure AD joined VMs. The option lets you add the VMs to an Azure AD security group based on their naming scheme. For more information, see Create a Microsoft Azure catalog.

Support for changing the storage type of existing VMs to a lower tier on shutdown in Azure environments. In Azure environments, you can now save storage costs by changing the storage type of existing VMs to a lower tier when the VMs are shut down. To do this, use the StorageTypeAtShutdown custom property. For more information, see Change the storage type of existing VMs to a lower tier on shutdown.

Support for allowing security identifiers while creating virtual machines. Previously, while creating new virtual machines with the configuration specified by a provisioning scheme, you could not add a security identifier (`ADAccountSid`) to the `NewProvVM` command. With this feature, you can now add the parameter `ADAccountSid` to uniquely identify the machines while creating new virtual machines. For more information, see Add SIDs while creating virtual machines.

Ability to get warnings associated with MCS catalogs. Previously, you did not get any information indicating that there are issues with your machine catalog. With this feature, you can now get warnings to understand issues with your MCS catalogs and fix those issues.

Warnings, unlike errors, do not cause an initiated provisioning task to fail.

To get warnings, use PowerShell commands. For more information, see Retrieve warnings associated with a catalog.

Shared tenants for connections. You can now add tenants and subscriptions that share the Azure Compute Gallery with the subscription of the connection. As a result, when creating or updating catalogs, you can select shared images from those tenants and subscriptions. For more information, see Edit connection settings.

Removed support for changing the OS type for Azure catalogs. When changing catalog images, only images with the same OS type as the image in use are shown. With this enhancement, Citrix DaaS no longer supports changing the OS type for Azure catalogs after catalog creation such as, changing from Windows OS type to Linux and vice versa.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 2023

New and enhanced features

Support for sharing images across different Azure tenants. Previously, in Azure environments, you could share images only with shared subscriptions using Azure Compute Gallery. With this feature, you can now select an image in Azure Compute Gallery that belongs to a different shared subscription in a different tenant to create and update an MCS catalog. For more information, see Image sharing across Azure tenants.

Policy modeling. The policy modeling feature is now generally available. You can simulate policies for planning and testing purposes. For more information, see Use the Policy Modeling wizard.

Ability to turn preview features on or off. In Full Configuration > Home, as a Citrix Cloud administrator with full access, you can now turn preview features on or off without contacting Citrix. For more information, see Home page for the Full Configuration interface.

Search Session Diagnostics with user name. This feature enables the use of Session Launch Diagnostics starting with the user name if you don't have the transaction id. This feature is specifically useful for help desk administrators to triage a failed session if the end user hasn't captured the transaction id. You can search for a user name, and select a session to triage from a list of failed sessions that the user attempted to launch over the last 48 hours. The Session Launch Diagnostics page shows the details of the failed session. It lists the exact component and stage where the failure occurred. For more information, see the Session Launch Diagnostics article.

Deploy secure web and SaaS apps with Secure Private Access. On the **Full Configuration > Applications > Applications** tab, a new option, **Add Web/SaaS Applications**, is now available in the action bar. The option lets you deploy secure web and SaaS apps with Secure Private Access. Citrix Secure Private Access provides an easy, flexible way for remote users to access web, SaaS, and client-server based apps using a Zero-Trust approach. It enables single sign-on to web and SaaS apps, along with granular security controls such as watermarking and copy/paste controls, among other security features. With Citrix Secure Private Access, you can combine all your virtualized and non-virtualized apps in one place and enhance the user experience for your users. See Citrix Secure Private Access.

Filter log content for a specific time duration. A new option, **Custom**, is now available in the time duration list in **Full Configuration > Logging > Events**. Use it to specify a period of the events for which you want to filter your search. For more information, see Configuration logging.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Updates for Autoscale. We've updated the **Control when Autoscale starts powering on tagged machines** option to make it easy to understand. The option controls when Autoscale starts powering on tagged machines based on the percentage of the remaining capacity of untagged machines. When the percentage falls below the threshold (default, 10%), Autoscale starts powering on tagged machines. When the percentage exceeds the threshold, Autoscale goes into power-off mode. For more information, see Autoscaling tagged machines (cloud burst).

App protection policies. You can now enable app protection when creating or editing a delivery group. The feature provides anti-keylogging and anti-screen-capturing capabilities for client sessions. For more information, see Create delivery groups and Manage delivery groups.

Real-time GPU Utilization available for AMD GPUs. You can now see GPU Utilization of AMD Radeon Instinct MI25 GPUs and AMD EPYC 7V12(Rome) CPUs on Monitor. Monitor already supports the NVIDIA Tesla M60 GPUs. GPU Utilization displays graphs with real-time percentage utilization of the GPU, the GPU memory, and of the Encoder and the Decoder to troubleshoot GPU-related issues on multi-session and single-session OS VDAs. The AMD GPU Utilization graphs are available only for VDAs running 64-bit Windows and Citrix Virtual Apps and Desktops 7 2212 or later. For more information, see GPU Utilization.

Support for scheduling configuration updates in Azure. In Azure environments, you can now schedule a time slot for the configuration updates of the existing MCS provisioned machines using the PowerShell command `Schedule-ProvVMUpdate`. Any power on or restart during the scheduled time slot applies a scheduled provisioning scheme update to a machine. You can also cancel the configuration update before the scheduled time using `Cancel-ProvVMUpdate`.

You can schedule and cancel the configuration update of:

- A single or multiple VMs
- An entire catalog

For more information, see Schedule configuration updates.

Support for using Citrix ready images directly from Google Cloud Marketplace. You can now browse and select images offered by Citrix on the Google Cloud Marketplace to create MCS catalogs. Currently, MCS supports only the machine profile workflow for this feature. For more information, see Google Cloud Marketplace.

Limit host groups scope in SCVMM Host Connection. Previously, host connection to SCVMM required the admin to have a single top level host group configured. This implies that the admin had visibility to all host groups, clusters, or hosts beneath the single top level host group. With this feature, in large deployments where a single SCVMM manages multiple clusters in different data

© 1997–2026 Citrix Systems, Inc. All rights reserved.

centers, you can now limit the host groups scope of the admins. To do this, you can use the Delegated Admin role in the Microsoft System Center Virtual Machine Manager (VMM) console to select the host groups to which an admin must have access. For more information, see Install and configure a hypervisor.

Support for zone-redundant storage in Azure. Previously, MCS offered only locally-redundant storage. With this feature, zone-redundant storage is now an option in Azure, allowing you to select a storage type depending on what type of redundancy you want to use. Zone-redundant storage replicates your Azure managed disk across multiple availability zones, which allows you to recover from a failure in one zone by utilizing the redundancy in others. For more information see, Enable zone-redundant storage.

January 2023

New and enhanced features

Option to downgrade storage disk to Standard HDD when VMs shut down. A new option, **Enable storage cost saving**, is now available on the **Disk Settings** page when you create or update Azure catalogs. The option saves storage costs by downgrading to Standard HDD for the storage disk and the write-back cache disk when the VM shuts down. The VM switches to its original settings on restart. For more information, see Create a Microsoft Azure catalog.

Support for configuring session roaming in Full Configuration. Previously, PowerShell was your only choice to configure session roaming for applications and desktops. You can now do that in **Full Configuration**. For more information, see Manage delivery groups.

Renamed some actions to better align with their actual meanings. We've renamed the following actions in **Full Configuration > Machine Catalogs** and **Full Configuration > Delivery Groups**. The workflows for performing those actions remain unchanged.

- **Update Machines** renamed to **Change Master Image**
- **Rollback Machine** Update renamed to **Roll Back Master Image**
- **Upgrade Catalog** renamed to **Change Functional Level**
- **Upgrade Delivery Group** renamed to **Change Functional Level**
- **Undo Upgrade Catalog** renamed to **Undo Functional Level Change**
- **Undo Upgrade Delivery Group** renamed to **Undo Functional Level Change**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for organizing application groups using folders. You can now create nested folders to organize application groups for easy access. For more information, see Organize application groups using folders.

Restriction enhancements for delivery groups. Previously, when restricting the use of apps or desktops for a delivery group, you could specify only users and user groups that were allowed to use them in a delivery group. You can now also add users and user groups that you want to block. This enhancement is useful when you add a group of users to an allow list and at the same time want to block a subset of users in the allow list. For more information, see Create delivery groups.

Access Citrix Analytics for Performance™ - Session Details from Monitor. The Session Details page from Citrix Analytics for Performance is now integrated in Monitor. Click **View Session Timeline** in the Sessions page in Monitor to view the Sessions Details page from Citrix Analytics for Performance within Monitor. This requires you to have a valid Citrix Analytics for Performance entitlement. The Session Details are available for sessions that are categorized as Excellent, Fair, or Poor in Citrix Analytics for Performance.

You can view a trend of the session experience for the session for up to the last three days along with the factors contributing to the experience. This information complements the live data available in Monitor, used by the helpdesk admin while troubleshooting issues related to session experience.

For more information, see the Site Analytics article.

Non-persistent VMs are deleted from hypervisors or cloud services when you delete them or their machine catalogs in Full Configuration. The option to retain VMs in hypervisors or cloud services is now available only to persistent VMs. For more information, see Manage machine catalogs.

December 2022

New and enhanced features

Support for creating Azure AD joined, Hybrid Azure AD joined, and Microsoft Intune enabled catalogs with Azure AD joined master VMs. You can now create Azure AD joined, Hybrid Azure AD joined, and Microsoft Intune enabled catalogs with Azure AD joined, Hybrid Azure AD joined, and non-domain-joined master VMs. If you want to manage a master VM by Microsoft Intune, use VDA version 2212 or later, and do not skip image preparation while creating or updating machine catalogs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on machine identities, see Azure Active Directory joined, Microsoft Intune, and Hybrid Azure Active Directory joined.

Support in MCS for deleting VM objects without accessing the hypervisor. You can now delete VM objects in MCS without having access to the hypervisor. When deleting a VM or provisioning scheme, MCS needs to remove tags so that the resources are no longer tracked or identified. Previously, if the hypervisor could not be accessed, the tag removal failures were ignored. With this feature, if the hypervisor is not accessible while using the `Remove-ProvVM` command the tag removal will fail, but by using the `PurgeDBOnly` option, you can still delete the VM resource object from the database. For more information, see Delete machines without hypervisor access.

November 2022

New and enhanced features

Support for delivering MSIX and MSIX app attach apps. In **Full Configuration > App Packages**, you can now upload MSIX and MSIX app attach packaged apps to Citrix Cloud, and deliver them to your users. For more information, see App packages.

Prompt for unsupported VDA versions and functional levels. The Full Configuration interface now alerts you about unsupported VDA versions and functional levels. To avoid potential issues:

- If a machine runs an unsupported VDA version, you are prompted to upgrade to a supported version.
- If the functional level of a catalog or delivery group is not supported, you are prompted to set it to a higher level.

TIP:

VDAs are covered by the CR and LTSR lifecycles of Citrix Virtual Apps and Desktops.

Ability to annotate master images extended to catalog creation. When creating an MCS catalog in **Full Configuration**, you can now annotate its master image. For more information, see Master image.

Support for exporting desktop assignment data through Full Configuration. When viewing desktop assignments for a single-session OS delivery group, you can now export the assignment data into a CSV file for auditing purposes. To do so, select such a delivery group in **Full**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration > Delivery Groups, go to the **Desktops** tab, and then click **Export** in the upper-left corner on the tab.

All Applications and Application Folders tabs consolidated into one. In **Full Configuration > Applications**, the **All Applications** and **Application Folders** tabs have been consolidated into one tab, **Applications**. This change unifies the user experience of folder view management across Full Configuration nodes.

Support for changing the storage type to a lower tier when a VM is shut down in Azure environments. In Azure environments, you can now save storage costs by switching the storage type of a managed disk to a lower tier when you shut down a VM. To do this, use the `StorageTypeAtShutdown` custom property. The storage type of the disk changes to a lower tier (as specified in the `StorageTypeAtShutdown` custom property) when you shut down the VM. After you power on the VM, the storage type changes back to the original storage type (as specified in `StorageType` or `WBCDiskStorageType` custom property). For more information, see Change the storage type to a lower tier when a VM is shut down.

Updates in Filters View. The Filters page in Monitor is updated to include separate Saved and Default filters lists for better visualization and accessibility to the filters. You can select a view from among Machines, sessions, Connections, or Application Instances. Then, you can select a filter from the list of Saved filters or Default filters to view the filtered list of data. You can use the drop-down lists to refine the filter criteria or edit existing criteria. You can save your filter in the Saved Filter list. For more information, see the Filters article.

Ability to reset the OS disk of a persistent VM in an MCS created machine catalog. In VMware virtualization environments, you can now use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. The feature automates the process of resetting the OS disk. For example, it helps in resetting the VM to its initial status of a persistent development desktop catalog created using MCS.

For more information on using PowerShell command to reset the OS disk, see Reset OS disk.

Support for updating machine profile and additional custom properties of MCS provisioned machines in Azure environments. Previously, in Azure environments, you could use `Request-ProvVMUpdate` to update `ServiceOffering` custom property of an MCS provisioned machine. Now, you can also update the machine profile and the following custom properties:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

For more information, see Update provisioned machines to current provisioning scheme state.

Support for machine profile in GCP. When you create a catalog to provision machines using Machine Creation Services (MCS) in Google Cloud Platform (GCP) environments, you can now use a machine profile to capture the hardware properties from a virtual machine and apply them to the newly provisioned VMs in the catalog. When `MachineProfile` parameter is not used, the hardware properties are captured from the master image VM or snapshot.

Machine profiles work with both Linux and Windows operating systems.

For information on how to create a machine catalog with a machine profile, see Create a machine catalog using a machine profile.

Support for updating MCS provisioned machines in GCP environments. In GCP environments, `Set-ProvScheme` changes the template (provisioning scheme) and does not affect existing machines. Using the PowerShell command `Request-ProvVMUpdate`, you can now apply the current provisioning scheme to an existing machine (or set of machines). Currently, in GCP, the property update supported by this feature is machine profile. For more information, see Update provisioned machines using PowerShell.

October 2022

New and enhanced features

Support for using machine profiles and host groups at the same time. When creating a catalog using an Azure Resource Manager master image, you can now use a machine profile and a host group at the same time. This is useful in scenarios where you want to use trusted launch for improved security and at the same time run the machines on dedicated hosts. For more information, see Microsoft Azure Resource Manager virtualization environments.

Support for organizing delivery groups using folders. You can now create a folder tree to organize delivery groups for easy access. For more information, see Organize delivery groups using folders.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for scheduling a one-time restart for machines through Full Configuration. A new option, **Once**, is now available when you create restart schedules for delivery groups. With this option, you can schedule machines in a delivery group to restart once, at a specified date and time. For more information, see Create a restart schedule.

Advanced Probe Scheduling. Improved scheduling of Application and Desktop Probes can now be done from Monitor. Using this feature, Citrix Probe Agent can be configured to run the probe tasks on specific days of the week and repeated at specified intervals during the day. This allows you to schedule a single probe task to repeat at specific times of the day and the week. You can now proactively check your site health with probes set to run regularly at suitable times. This feature simplifies probe setup and management in Monitor. For more information, see Application and Desktop Probing.

September 2022

New and enhanced features

Older versions of the Remote PowerShell SDK are now deprecated. If you are using a deprecated version, the SDK stops working and you see an error message prompting you to download the current version. If this happens, download the latest Remote PowerShell SDK from the Citrix website.

Machine catalogs with Trusted launch in Azure. In Azure environments, you can create machine catalogs enabled with Trusted launch, and use the `SupportsTrustedLaunch` property of the VM inventory to determine the VM sizes that support Trusted launch.

Trusted launch is a seamless way to improve the security of Generation 2 VMs. Trusted launch protects against advanced and persistent attack techniques. For more information, see Machine catalogs with Trusted launch.

Support for identifying Microsoft System Center Virtual Machine Manager resources created by MCS. You can now identify Microsoft System Center Virtual Machine Manager (SCVMM) resources created by MCS using tags. For more information on the tags that MCS adds to the resources, see Identify resources created by MCS.

Support for identifying VMware resources created by MCS. You can now identify VMware resources created by MCS using tags. For more information on the tags that MCS adds to the resources, see Identify resources created by MCS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for optimizing AWS Workspace throttling. You can now power on and off a large number of machines in an AWS Workspace without encountering throttling issues. Throttling issues occur when the number of requests sent to AWS Workspace exceeds the number of requests that the server can handle. Therefore, Citrix now groups multiple requests into one single request before sending it to the AWS Workspace SDK.

Ability to check machine details when viewing machine counts in Home. When viewing machine counts by availability state in **Home**, you can now click a state to view details of machines in that state. For more information, see Home page for the Full Configuration interface.

Support for machine catalog creation using an image from a different subscription in the same Azure tenant. Previously, in Azure environments, you could only select an image within your subscription to create a machine catalog. With this feature, you can now select an image in Azure Compute Gallery (formerly Shared Imaged Gallery) that belongs to a different shared subscription to create and update MCS catalogs.

For more information on creating a catalog, see Create a machine catalog using an Azure Resource Manager image.

For information on sharing image with another service principal in the same tenant, see Image sharing with another service principal in the same tenant.

For information on PowerShell commands to select an image from a different subscription, see Using PowerShell to select an image from a different subscription.

For more information on Azure Compute Gallery, see Azure Shared Image Gallery.

August 2022

New and enhanced features

Support for identifying Citrix hypervisor resources created by MCS. You can now identify Citrix hypervisor resources created by MCS using tags. For more information on the tags that MCS adds to the resources, see Identify resources created by MCS.

Support for using host groups and Azure availability zones at the same time. In Azure environments, there is now a pre-flight check to assess whether the creation of a machine catalog will be successful based on the Azure availability zone specified in the custom property and the host group's zone. Catalog creation fails if the availability zone custom property does not match the host group's zone.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A host group is a resource that represents a collection of dedicated hosts. A dedicated host is a service that provides physical servers that host one or more virtual machines. Azure availability zones are physically separate locations within each Azure region that are tolerant to local failures.

For more information on the various combinations of availability zone and host group zone that result in successful or failed the machine catalog creation, see Using host groups and Azure availability zones at the same time.

Support for updating the folder ID of a machine catalog in VMware. In VMware virtualization environments, you can now update the folder ID of an MCS machine catalog using the custom property `FolderID` in `Set-ProvScheme`. The VMs created after updating the folder ID are created under this new folder ID. If this property is not specified in `CustomProperties`, then VMs are created under the folder where the master image is located. For more information on updating the folder ID, see Update the folder ID of a machine catalog.

Time zone setup. You can now configure the date and time format of the interface to suit your preferences using the **Date and time** setting. For more information, see Time zone setup.

Image Portability Service (IPS) now supports Amazon Web Services (AWS). By configuring the required permissions and components for AWS, IPS workflows can be used with an AWS account. See Migrate workloads to public cloud for more details.

Page file setting during image preparation in Azure environments. In Azure environments, you can now avoid potential confusion with the page file location. To that end, MCS now determines the page file location when you create the provisioning scheme during image preparation. This calculation is based on certain rules. Features like ephemeral OS disk (EOS) and MCS I/O have their own, expected page file location, and are exclusive to each other. Also, if you decouple image preparation from provisioning scheme creation, MCS correctly determines the page file location. For more information on page file location, see Page file location.

Support for updating page file setting in Azure environments. While creating a catalog in an Azure environment, you can now specify the page file setting, including its location and the size, using PowerShell commands. This overrides the page file setting determined by MCS. You can do this by running the `New-ProvScheme` command with the following custom properties:

- `PageFileDiskDriveLetterOverride`: Page file location disk drive letter
- `InitialPageFileSizeInMB`: Initial page file size in MB
- `MaxPageFileSizeInMB`: Maximum page file size in MB

For more information on updating the page file setting, see Update page file setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Updates to the Home page. The Get Started widget now has a new look and feel. Other updates to the Home page include:

- The newly added Refresh and Help icons in the upper right corner.
- Clickable resource counts, providing quick access to relevant resource pages.
- Enhancement to the Dislike icon. If you dislike a recommendation, the recommendation disappears. If you dislike the recommendation widget, the widget disappears.

For more information, see Home page.

Support for enabling Azure VM extensions. When using an ARM template spec as a machine profile to create a machine catalog, you can now add Azure VM extensions to the VMs in the catalog, view the list of supported extensions, and remove extensions you added. Azure VM extensions are small applications that provide post-deployment configuration and automation tasks on Azure VMs. For example, if a VM requires software installation, antivirus protection, or the ability to run a script inside it, you can use a VM extension. For more information on how to enable Azure VM extensions, see Use PowerShell to enable Azure VM extensions.

Trusted launch support for ephemeral OS disk. You can now create provisioning schemes using ephemeral OS disk on Windows with trusted launch. Trusted launch is a seamless way to improve the security of generation 2 VMs. It protects against advanced and persistent attack techniques by combining technologies that can be independently enabled like secure boot and virtualized version of trusted platform module (vTPM). For more information on creating a machine catalog, see Create a machine catalog using an Azure Resource Manager image.

July 2022

New and enhanced features

Dynamic session timeouts for single-session OS machines. Dynamic session timeouts now support single-session OS machines. A delivery group with at least one VDA of version 2206 or later is required. Ensure that those VDAs have registered with Citrix Cloud at least once. For more information, go to Dynamic session timeouts.

Send logoff reminders without forcing user logoff in Autoscale. A new feature is now available in **User Logoff Notifications** (formerly **Force User Logoff**) in Autoscale. The feature lets you send logoff reminders to users without forcing them to log off. Doing that avoids potential data loss caused by forcing users to log off from their sessions. See User logoff notifications for details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ability to set the Linux OS license type when creating Linux VM catalogs in Azure. Using the Full Configuration interface, you can now choose the Linux OS license type when creating Linux VM catalogs in Azure. You have two choices for bring-your-own Linux licenses: Red Hat Enterprise Linux and SUSE Linux Enterprise Server. For more information, see Create a machine catalog using an Azure Resource Manager image.

Enhanced search experience in Full Configuration. The Search node provides the following new features and enhancements:

- **Ability to export search results**. You can now export search results. To do that, click the export icon in the upper right corner.
- **New filter available**. A filter, Pending Power Action, is now available for use. Use the filter to refine your search.
- **"Does not contain" search support for certain items**. Items such as machine names and tags now support "Does not contain" search criteria.
- **Support for searching for objects when adding filters**. When adding filters for the following objects, you can now search for them: connections, machine catalogs, delivery groups, application groups, and tags.

For more information, see Use Search in the Full Configuration management interface.

Support for VMware Storage Profiles. When you create a machine catalog using a master image on a vSAN Datastore, you can now copy the storage policy such as the RAID-1 or RAID-5 information from the master image to the created target devices. For existing catalogs, the storage policy remains unchanged even if you update the catalog.

Support for RestrictedKrbHost SPN registration. All the Citrix MCS created computer accounts are now registered with `RestrictedKrbHost` Service Principal Names (SPN). This avoids the requirement to run the `setspn` command to register the SPN for the computer accounts after MCS creates them.

App Packages in Full Configuration for delivering Microsoft packaged applications. The App-V node is renamed to App Packages and redesigned to accommodate more types of Microsoft packaged apps. Previously, you had to use the discovery module to add App-V packaged apps to your environment for delivery. You can now add and deliver the apps in one place by using the App Packages node. For more information, see App packages.

Support for using ARM template specs as machine profiles. Previously, you could use only VMs as machine profiles. You can now use ARM template specs as machine profiles as well when creating Azure machine catalogs. This feature lets you take advantage of Azure ARM template

© 1997–2026 Citrix Systems, Inc. All rights reserved.

features such as versioning. To ensure that the selected spec is configured correctly and contains required configurations, we perform validation on it. If the validation fails, you are prompted to select a different machine profile. For more information, see Create a machine catalog using an Azure Resource Manager image.

Support for validating ARM template spec. You can now validate the ARM template spec to make sure that it can be used as a machine profile to create a machine catalog. There are two ways to validate the ARM template spec:

- Using the Full Configuration management interface.
- Using the PowerShell command.

For more information on validating the ARM template spec, see Create a machine catalog using an Azure Resource Manager image.

June 2022

New and enhanced features

Restart schedule support for single-session OS machines. Previously, the restart schedule feature was available only for multi-session OS machines. It's now also available for single-session OS machines. You can now create restart schedules for delivery groups containing single-session OS machines. For more information, see Create and manage restart schedules for machines in a delivery group.

Option to perform user name pre-checks. An option, **Check name**, is now available when you enter domain credentials. With the option, you can check whether the user name is valid or unique. The option is useful, for example, when:

- The same user name exists in multiple domains. You are prompted to select the desired user.
- You can't remember the domain name. You can enter the user name without specifying the domain name. If the check passes, the domain name populates automatically.

For more information, see Domain credentials.

Ability to change the network setting for an existing provisioning scheme. You can now change the network setting for an existing provisioning scheme so that the new VMs are created on the new subnetwork. Use the parameter `-NetworkMapping` in the `Set-ProvScheme` command to change the network setting. Only the newly provisioned VMs from the scheme will have the new subnetwork settings. You must also make sure that the subnetworks are under the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

same hosting unit. For more information, see Change the network setting for an existing provisioning scheme.

Retrieve region name information for Azure VMs, managed disks, snapshots, Azure VHD, and ARM template. You can now display the region name information for an Azure VM, managed disks, snapshots, Azure VHD, and ARM template. This information is displayed for the resources on the master image when a machine catalog is assigned. For more information, see Retrieve region name information for Azure VMs, managed disks, snapshots, Azure VHD, and ARM template.

Ability to use machine profile property values in Azure environment. While creating an Azure catalog with a machine profile, you can now set the property values from the ARM template spec or VM, whichever is used as a machine profile, if the values are not explicitly defined in the custom properties. The properties affected by this feature are:

- Availability zone
- Dedicated Host Group Id
- Disk Encryption Set Id
- OS type
- License type
- Service Offering
- Storage type

If some of the properties are missing from the machine profile and not defined in the custom properties, then the default value of the properties takes place wherever applicable. For more information, see Use machine profile property values.

Extended support for VDA upgrade. Using the Full Configuration interface, you can now upgrade MCS-provisioned persistent machines. You can upgrade them on a per-catalog or a per-machine basis. For more information, see Upgrade VDAs using the Full Configuration interface.

Citrix Probe Agent in Citrix Cloud Japan and Citrix Cloud Government Control Planes. Citrix Probe Agent now supports sites hosted on Citrix Cloud Japan and Citrix Cloud Government Control Planes. To use the probing agent in these planes, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" to 2 for Japan and 3 for the Government region. Citrix Probe Agent automates the process of checking the health of virtual apps and desktops that are published in a site. For more information, see Application and Desktop Probing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customize the port used for communication between VDAs and Cloud Connectors. You can now customize the port that the VDA uses to communicate with Cloud Connectors based on your specific security requirements. This feature is useful if your security team doesn't allow the default port (port 80) to be open or if the default port is already in use. For more information, see Customize the port for communicating with Cloud Connectors.

Support for organizing machine catalogs using folders. You can now create nested folders to organize machine catalogs for easy access. For more information, see Organize catalogs using folders.

Support for SCVMM 2022. Citrix DaaS now supports Microsoft's System Center Virtual Machine Manager (SCVMM) 2022. SCVMM provides a range of services to include maintaining the resources you need to deploy VMs. For more information about the new features supported in SCVMM 2022, see What's new in System Center Virtual Machine Manager.

Support for configuring maximum concurrent provisioning operations parameter on AWS. Citrix DaaS now supports `MaximumConcurrentProvisioningOperations` as a configurable custom property for MCS on AWS. `MaximumConcurrentProvisioningOperations` is the property that determines the number of VMs you can create or delete simultaneously. While MCS supports 100 maximum concurrent provisioning operations by default, you can now enter PowerShell commands to customize this value. You can enter a range from 1-1000. Setting this property to your preferred value allows you to control the number of parallel tasks you can perform when creating or deleting VMs. For details about configuring the maximum concurrent provisioning operations, see Host Connection Default Values.

May 2022

New and enhanced features

Enhanced Session launch diagnostics. Citrix DaaS now supports detailed session launch failure diagnostics. You can now view the components involved in the session launch sequence. The components which failed with last generated error codes are highlighted. This helps identify the exact reason for a session launch failure and take the recommended action.

The Transaction page is extended with the Transaction Details panel that contains a list of components indicating the error occurrence. Clicking on the component name displays the Component Details and the Last Known Failure Details. The Failure Reason and Error Code are displayed. Clicking the Learn more link leads to the specific code on Error codes containing a detailed description and recommended action. For more information, see Session Diagnostics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for using Set-ProvServiceConfigurationData in Remote PowerShell SDK. You can now run `Set-ProvServiceConfigurationData` using Remote PowerShell SDK to do the settings on all applicable parameters. You can also skip enabling DHCP during image preparation using this command. Following is the list of settings that is supported with `Set-ProvServiceConfigurationData`:

- Change Image Preparation Timeout: `Set-ProvServiceConfigurationData -Name "ImageManagementPrep_PreparationTimeout" -value 60`
- Skip Enable DHCP: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value EnableDHCP`
- Skip Microsoft Windows KMS Rearm: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm`
- Skip Microsoft Office KMS Rearm: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OfficeRearm`
- Disable preparation VM auto shutdown: `Set-ProvServiceConfigurationData –Name ImageManagementPrep_NoAutoShutdown –Value true`
- Disable domain injection: `Set-ProvServiceConfigurationData –Name DisableDomainInjection –Value true`

Ability to set the Linux license type when creating Linux machine catalogs using PowerShell commands. Using PowerShell commands, you can set the Linux license type when creating Linux machine catalogs. You have two choices for bring-your-own Linux licenses: RHEL_BYOS and SLES_BYOS. The setting defaults to Azure Linux licensing. For more information, see Create a machine catalog using an Azure Resource Manager image.

Support for identifying all Azure resources created by MCS. You can now identify all Azure resources created by MCS such as Image, ID disk, OS disk, NIC, VM, and so on that are associated with a ProvScheme using a tag called `provschemeID`. For more information on the tags that MCS adds to the resources, see Identify resources created by MCS.

Support for adding non-Active Directory users manually. Using the Full Configuration management interface, you can now enter a semicolon-separated list of user names when adding non-Active Directory users for a catalog. Consider the format when adding users that reside in different directories. For example, if the users are in Active Directory, enter the names directly. If not, enter the names in this format: `<identity provider>:<user name>`. Example: `AzureAD:username`. For more information, see Create machine catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 2022

New and enhanced features

Home page for the Full Configuration interface. Full Configuration now has a home page, which provides an overview of your Citrix DaaS deployment and workloads along with information that helps you get the most from your subscription. The page comprises the following parts:

- **Service overview**. Provides an overview of your Citrix DaaS deployment and workloads.
- **Recommendations**. Recommends features that are available with your subscription and collects your feedback.
- **What's new**. Shows the latest features.
- **Preview features**. Shows features that are currently in preview.
- **Get started**. Shows steps to guide you through the initial setup.

For more information, see Home page.

Show the progress of catalog creation and updates. Full Configuration now lets you stay up to date on catalog creation and updates. You can gain an overview of the creation and update process, view the history of steps performed, and monitor the progress and running time of the current step. For more information, see Start creating the catalog.

Display available hypervisors and cloud services based on the selected zone. In Full Configuration, when creating hosting connections, you're required to select a zone before selecting a connection type. The Connection type drop-down list displays hypervisors and cloud services available with the zone. Previously, to ensure the Connection type list shows a required hypervisor or cloud service, you had to install its plug-in in every zone. With this new configuration sequence, you can now install the plug-in only in the required zone.

You can also use PowerShell command to get the list of hypervisor plug-in available with the selected zone. For more information, see Create a connection and resources.

Support for non-on-premises-AD-joined users in Full Configuration. A new field, **Select identity type**, is available in the interfaces where you assign users to provisioned desktops or apps, delivery groups, or application groups. With the field, you can now select user accounts from any of the following identity providers to which your Citrix Cloud is connected:

- Active Directory
- Azure Active Directory
- Okta

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ability to reject invalid custom properties in Google Cloud Platform (GCP) and Azure environments. You can now avoid potential confusion if custom properties set at `New-ProvScheme` and `Set-ProvScheme` do not take effect. If you specify non-existing custom property or properties, you get an error message. For more information, see Important consideration about setting custom properties.

Support for creating Azure Active Directory joined machines. In **Full Configuration**, when you create a catalog, an **Azure Active Directory joined** identity type, is now available in **Machine Identities**. With that identity type, you can use MCS to create machines that are joined to Azure Active Directory. You also have an extra option, **Enroll the machines in Microsoft Intune**, to enroll the machines in Microsoft Intune for management.

For information about creating Azure Active Directory joined catalogs, see Create machine catalogs. For information about requirements and considerations related to Azure Active Directory join, see Azure Active Directory joined.

Support for creating hybrid Azure Active Directory joined machines. In **Full Configuration**, when you create a catalog, a **Hybrid Azure Active Directory joined** identity type, is now available in **Machine Identities**. With that identity type, you can use MCS to create hybrid Azure Active Directory joined machines. Those machines are owned by an organization and signed into with an Active Directory Domain Services account that belongs to that organization.

For information about creating hybrid Azure Active Directory joined catalogs, see Create machine catalogs. For information about requirements and considerations related to hybrid Azure Active Directory join, see Hybrid Azure Active Directory joined.

Azure trusted launch support for snapshots. In addition to images, Azure trusted launch is now available for snapshots as well. If you select a snapshot with trusted launch enabled, using a machine profile is mandatory. Also, you must select a machine profile with trusted launch enabled. For more information, see Microsoft Azure Resource Manager cloud environments.

Export machines. You can now export machines listed on the **Machines** page of the **Machine Catalog Setup** wizard to a CSV file, to be used as a template when adding machines to a catalog in bulk. For more information, see Export machines from a catalog.

Option to access Workspace Environment Management web console. An option, Environment Management (Web), is now available in the menu of the **Manage** tab. The option takes you to the new, web-based Workspace Environment Management console. To access the legacy console, use **Environment Management**. We are in the process of migrating the full set of functionalities

© 1997–2026 Citrix Systems, Inc. All rights reserved.

from the legacy console to the web console. The web console generally responds faster than the legacy console. For more information, see Workspace Environment Management service.

Ability to manage ProvScheme parameters. When you use MCS to create a catalog, you will now get an error if you set the `New-ProvScheme` parameters in unsupported hypervisors during machine catalog creation or update `Set-ProvScheme` parameters after machine catalog is created. For more information, see Create machine catalogs.

Increased resource location limits. Resource location limits for single-session VDAs and multi-session VDAs are now increased to 10000 and 1000 respectively. For more information, see Limits.

Support for restarting non-power managed machines after draining all sessions. Citrix DaaS now allows you to create restart schedules for machines that are not power managed after all sessions are drained from the machines. In the Full Configuration interface, select **Restart all machines after draining all sessions** as the **Restart duration**. For more information, see Create a restart schedule.

Support for upgrading VDA machines (preview). Using the Full Configuration interface, you can now upgrade VDA machines for your Citrix DaaS deployment. You can upgrade them on a per-catalog or a per-machine basis. The feature applies to machines that are not created using MCS (for example, physical machines). For more information, see Upgrade VDAs using the Full Configuration interface.

Machines are not shut down during outages. Citrix DaaS now prevent virtual machines from being shut down by the broker when the zone that the machines are in experiences an outage. The machines automatically become available for connections when the outage ends. You don't have to take any action to make the machines available after the outage.

Session launch diagnostics. Citrix DaaS now supports enhanced session launch failure diagnostics. Use the Citrix Workspace app-generated 32-digit (8-4-4-4-12) Transaction ID from inside Citrix Monitor (that is, Citrix Director service) to narrow down to the exact component and stage where the problem occurred and apply the recommended actions to resolve the issue. For more information, see Session launch diagnostics.

Option to access the Session Recording service. An option, Session Recording, is now available in the menu of the **Manage** tab. The introduction of the Session Recording service provides centralized management of policies, playback, and server configurations. It eases the burden on IT administrators by providing a unified entry point to manage and observe the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

distributed objects across your organization. For more information, see Session Recording service (preview).

Rebranded Citrix Virtual Apps and Desktops service. **Citrix Virtual Apps and Desktops service** has been renamed to **Citrix DaaS**. Learn more about the name change at our announcement on our blog.

The following offerings of Citrix Virtual Apps and Desktops service have been renamed.

- **Citrix Virtual Apps service Advanced** renamed to **Citrix DaaS Advanced**.
- **Citrix Virtual Apps service Premium** renamed to **Citrix DaaS Premium**.
- **Citrix Virtual Desktops™ service** renamed to **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops service Advanced** renamed to **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops service Premium** now available as **Citrix DaaS Premium and Citrix DaaS Premium Plus**.
- **Citrix Virtual Apps and Desktops Standard for Azure** renamed to **Citrix DaaS Standard for Azure**.
- **Citrix Virtual Apps and Desktops Standard for Google Cloud** renamed to **Citrix DaaS Standard for Google Cloud**.
- **Citrix Virtual Apps and Desktops Premium for Google Cloud** renamed to **Citrix DaaS Premium for Google Cloud**.

Implementing this transition in our products and their documentation is an ongoing process. Your patience during this transition is appreciated.

- The product UI, in-product content, and the images and instructions in product documentation will be updated in the coming weeks.
- It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.
- Related product documentation and other resources (such as videos and blog posts) that are linked from this product documentation might still contain former names.

NOTE:

The on-premises **Citrix Virtual Apps and Desktops** product name remains the same.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

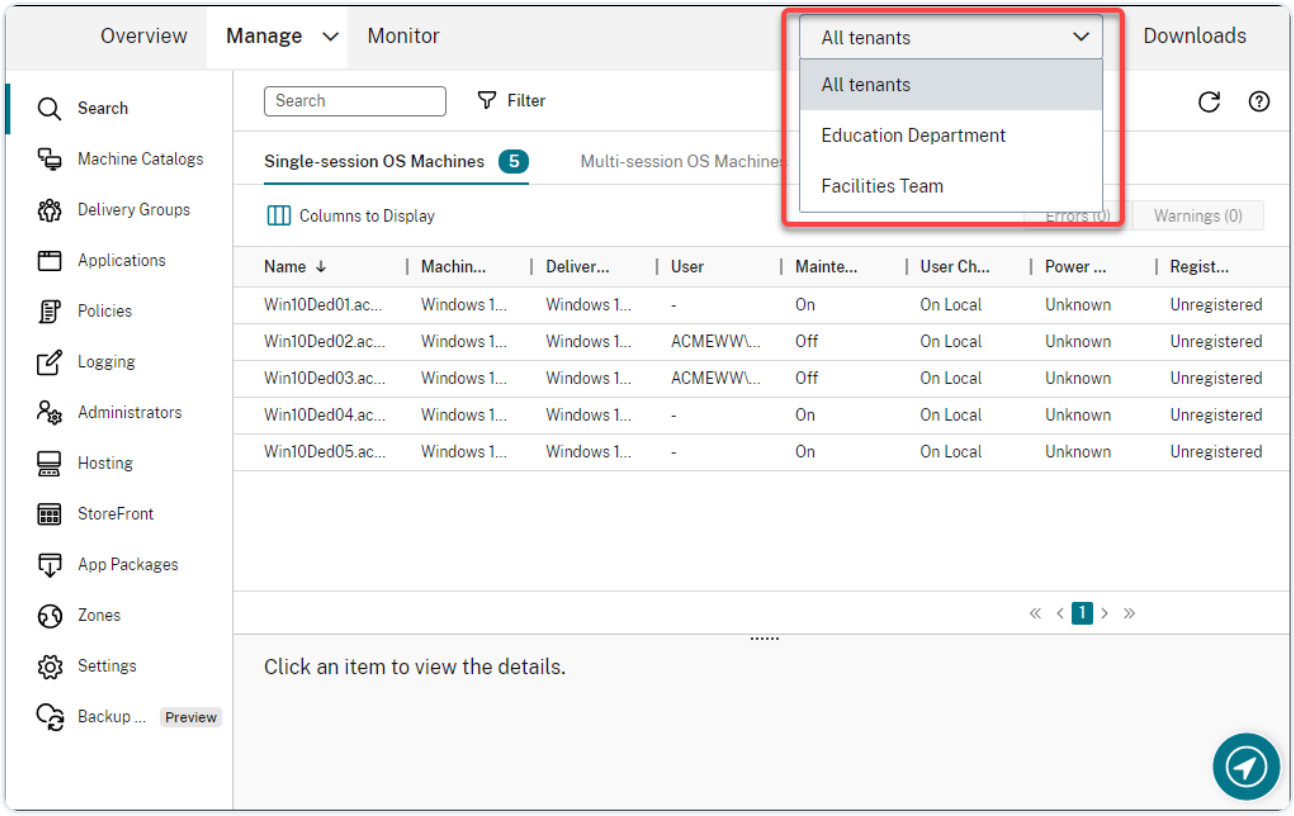
Tenant support in Full Configuration. You can now create configuration partitions within a single Citrix DaaS instance. You achieve that by creating tenant scopes in **Administrators > Scopes** and associating related configuration objects, such as machine catalogs and delivery groups, with those tenants. As a result, administrators with access to a tenant can manage only objects that are associated with the tenant. This feature is useful, for example, if your organization:

- Has different business silos (independent divisions or separate IT management teams) or
- Has multiple on-premises sites and wants to maintain the same setup in a single Citrix DaaS instance.

Also, the Full Configuration interface lets you filter tenant customers by name. By default, the interface displays information about all tenants.

The feature is available for both Citrix Service Providers (CSPs) and non-CSPs. The interface in a CSP environment is essentially the same as that in a non-CSP environment except for the method used to create tenants.

- CSPs onboard tenant customers to Citrix DaaS and then configure administrator access to Citrix DaaS. For more information, see Citrix DaaS for Citrix Service Providers.
- Non-CSPs create tenant customers by first creating scopes and then configuring custom access for respective administrators. For more information, see Create and manage scopes.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Updates for Autoscale. We have updated Autoscale with a blade style to bring you a better user experience. The workflows for configuring your settings remain the same. Other updates to Autoscale include:

- Renamed **Restrict Autoscale** to **Autoscaling Tagged Machines** to make it easy to understand.
- Added a new option, **Control when Autoscale starts powering on tagged machines**. The option lets you control when Autoscale starts powering on tagged machines based on the usage of untagged machines.

For more information on autoscaling tagged machines, see Autoscale tagged machines.

License validity checks. The Full Configuration interface now automatically checks the validity of licenses in use by host connections. A host connection is placed into maintenance mode if its license is invalid. As a result, you cannot perform certain operations, such as editing the connection and turning off maintenance mode. A license becomes invalid, for example, when:

- The license has expired. In this case, contact your Citrix sales representative to renew it or to purchase new licenses.
- The license has been deleted from the License Server.

Blade style applied to the Machine Catalogs and Policies nodes. Blade styles are now applied to all nodes of Full Configuration.

Support for updating MCS provisioned machines in Azure environments. `Set-ProvScheme` changes the template (provisioning scheme) and does not affect existing machines. Using Request-ProvVMUpdate command, you can now apply the current provisioning scheme to an existing machine (or set of machines). Currently, the property update supported by this feature is `ServiceOffering`. For more information, see Update provisioned machines to current provisioning scheme state.

March 2022

New and enhanced features

Citrix Virtual Apps and Desktops for Google Cloud available on Google Cloud Marketplace. Citrix Virtual Apps and Desktops Premium for Google Cloud is now available for purchase on Google Cloud Marketplace. Citrix Virtual Apps and Desktops Premium for Google Cloud runs the Citrix Virtual Apps and Desktops service control plane on Google Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure trusted launch support. Azure trusted launch is now available for the Full Configuration management interface. If you choose to select an image with trusted launch enabled, using a machine profile is mandatory. Also, you must select a machine profile with trusted launch enabled. For more information, see Microsoft Azure Resource Manager cloud environments.

Blade style applied to wizards in three more nodes in Full Configuration. The nodes are **Search**, **Delivery Groups**, and **Applications**.

Image Portability Service (IPS) has been released for general availability. IPS simplifies the management of images across platforms. This feature is useful for managing images between an on-premises Resource Location and the public cloud. The Citrix Virtual Apps and Desktops REST APIs can be used to automate the administration of resources within a Citrix Virtual Apps and Desktops site. For more information, see Migrate workloads to public cloud.

February 2022

New and enhanced features

Azure permissions. There are two sets of permissions required for security requirements and to minimize risk.

- Minimum permissions: This set of permissions gives better security control. However, new features that require additional permissions will fail because of using minimum permissions.
- General permissions: This set of permissions does not block you from getting new enhancement benefit.

For more information, see About Azure permissions.

Support for using VM's temporary disk to host the write-back cache disk in Azure environments. We added an option, **Use non-persistent write-back cache disk**, to the **Machine Catalog Setup > Disk Settings** page of the **Manage > Full Configuration** interface. Select that option if you do not want the write-back cache disk to persist for the provisioned VMs. With the option selected, we use the VM's temporary disk to host the write-back cache disk if the temporary disk has sufficient space. Doing that reduces your costs. For more information, see Microsoft Azure Resource Manager cloud environments.

Updates to AWS host connection default settings. The AWS host connection default setting values are updated to higher values and most likely same for all AWS cloud platform setup. This helps to create host connections in AWS cloud environments, without evaluating and configuring

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the default setting values according to individual setup. For more information, see Host connection default values.

Added support for different storage tiers in GCP environments. You can now provide the following custom properties in the GCP environments to set the storage type of the disks attached to the newly created VM:

- StorageType
- IdentityDiskStorageType
- WBCDiskStorageType

For more information, see Citrix Virtual Apps and Desktops Service SDK.

Change certain VM settings after creating Azure VM catalogs. Using the Full Configuration management interface, you can now change the following settings after creating a catalog:

- Machine size
- Availability zones
- Machine profile
- Windows licenses

To do that, on the **Machine Catalogs** node, select the catalog and then select **Edit Machine Catalog** in the action bar. For more information, see Edit a catalog.

Support for storing Azure ephemeral OS disk either on the cache disk or temporary disk. Citrix Virtual Apps and Desktops service now allows you to store the Azure ephemeral OS disk either on cache disk or temporary disk for an Azure-enabled virtual machine. This functionality is useful for Azure environments that require a higher performant SSD disk over a standard HDD disk. For more information, see Microsoft Azure Resource Manager cloud environments.

Support for Nutanix clusters on AWS. Citrix Virtual Apps and Desktops service supports Nutanix Clusters on AWS. Nutanix Clusters simplifies how applications are run on private or multiple public clouds. For more information, see Nutanix clusters on AWS.

Support for VMware cloud on Amazon Web Services (AWS). VMware cloud on Amazon Web Services (AWS) enables you to migrate VMware based on-premises Citrix workloads to AWS cloud and your core Citrix Virtual Apps and Desktops environment to Citrix Virtual Apps and Desktops service. For more information, see VMware cloud on Amazon Web Services (AWS).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for configuring write-back cache disk for machines running on Google Cloud Platform (GCP). In the Full Configuration management interface, when provisioning machines on GCP, you can now configure the following write-back cache disk settings:

- Disk size
- Memory allocated to cache
- Disk storage type
- Disk persistence

For more information, see Create a machine catalog in the Google Cloud Platform virtualization environments article.

January 2022

New and enhanced features

Support for Nutanix clusters on AWS. Citrix Virtual Apps and Desktops service now supports Nutanix clusters on AWS. This support provides the same functionality as a Nutanix on-premises cluster. Only a single cluster is supported, *Prism Element*. For more information, see Nutanix virtualization environments.

New features available in Cloud Health Check. Cloud Health Check has been updated to a new version with features including:

- **Automatic fix.** Cloud Health Check now supports automatically detecting and fixing certain issues identified on machines where it is running. There is now a results report to show you what specific actions were taken. For more information, see Automatic fix.
- **Command line support.** Cloud Health Check can now be run from the command line. For more information, see Running Cloud Health Check on the command line.
- **Citrix Universal™ Injection Driver status.** Cloud Health Check now shows the Citrix UVI driver status and has a related event log check for Citrix UVI drivers.
- **Session launch registry check.** Cloud Health check now checks for session launch registry settings.
- **Updates to check report.** For checked items that have several check points, the final check report now lists all the checks that have been verified to show what actions were performed during the health check.

For more information, see Cloud Health Check.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot VDA registration and session launch issues using Full Configuration. Using the Full Configuration management interface, you can now run checks that gauge the health of VDAs. VDA health checks identify possible causes for common VDA registration and session launch issues. You can run health checks individually and in batches. For more information, see VDA health checks.

Ability to specify the Azure secret expiration date for existing connections. Using the Full Configuration management interface, you can now specify the date after which the application secret expires. For guidance on how to view the expiration date of the secret, see Microsoft Azure Resource Manager cloud environments. When using this feature, consider the following differences:

- For service principals created manually in Azure, you can directly edit the expiration date on the **Edit Connection > Connection Properties** page.
- For first-time edits of the expiration date for service principals created through Full Configuration on your behalf, go to **Edit Connection > Edit settings > Use existing**. You can make subsequent edits on the **Edit Connection > Connection Properties** page.

A button to add administrators. We added a button, **Add Administrator**, to the **Full Configuration > Administrators > Administrators** tab. The button offers a quick way to go to **Identity and Access Management > Administrators**, where you can add (invite) administrators. For more information, see Add an administrator.

New look and feel of wizards in Full Configuration. We have updated the wizards in the following nodes with a new style, including colors, fonts, and other formatting changes, to bring you a better user experience: **Administrators**, **Hosting**, **StoreFront**, **App Packages**, **Zones**, and **Settings**. The new wizards appear in blade views with wider viewports, enabling more content to display. The workflows for configuring your settings remain the same.

Support for retaining system disk when MCS I/O is enabled for machines running on Google Cloud Platform (GCP). In the Full Configuration management interface, when provisioning machines on GCP, you can now retain system disk during power cycles when MCS storage optimization (MCS I/O) is enabled. For more information, see Enabling MCS storage optimization updates.

Support for direct upload or download from EBS on Amazon Web Services (AWS). AWS now provides API to allow direct creation of EBS volume with desired content. You can now use the API to eliminate volume worker requirement for catalog creation and VM addition. For information on AWS permissions required for this functionality, see Amazon Web Services cloud environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ability to identify Amazon Web Services (AWS) resources created by MCS. We added a new tag named `CitrixProvisioningSchemeID` to identify AWS resources created by MCS. For more information, see Identify resources created by MCS.

Ability to configure access to Manage and Monitor. The Full Configuration management interface now provides you with additional options to control whether to grant custom roles access to **Manage** and **Monitor**. For more information, see Create and manage roles.

December 2021

New and enhanced features

Support for Google Cloud VMware Engine. The platform now enables you to migrate VMware based on-premises Citrix workloads to Google Cloud and your core Citrix Virtual Apps and Desktops environment to Citrix Virtual Apps and Desktops service. For more information, see Google Cloud Platform (GCP) VMware Engine support.

Ability to specify what account names start with when specifying a naming scheme. This release introduces an option to the **Machine Catalog Setup > Machine Identities** page of the Full Configuration management interface. The option lets you specify numbers or letters the account names start with, giving you more control over how machine accounts are named during catalog creation. For more information, see Machine identities.

Support for creating Nutanix AHV XI and Nutanix AHV Prism Central (PC) connections. In the Full Configuration management interface, you can now create Nutanix AHV XI and Nutanix AHV PC connections. For more information, see Nutanix virtualization environments.

Support for selecting the storage type for OS disks when provisioning VMs on GCP. In the Full Configuration management interface, when provisioning VMs on GCP, you can now select the storage type for the OS disk. Available storage options on the **Machine Catalog Setup > Storage** page include **Standard persistent disk**, **Balanced persistent disk**, and **SSD persistent disk**. For more information, see Create a machine catalog.

Full Configuration management interface now supports Azure ephemeral disk. Previously, PowerShell was your only choice to create machines that used ephemeral OS disks. We now add an option, **Azure ephemeral OS disk**, to the **Machine Catalog Setup > Storage and License Types** page. Select the option if you want to use the VM's local disk to host the operating system disk. For more information, see Create a machine catalog using an Azure Resource Manager image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Protect Machine Creation Services (MCS) managed resources from accidental deletion. You can now protect MCS managed resources on the Google Cloud Platform (GCP) by applying GCP's `deletionProtection` flag enabled for the VMs. Using the `compute.instances.setDeletionProtection` permission or the IAM Compute Admin role, you can reset the flag to allow the resource to be deleted. This functionality is applicable for both persistent and non-persistent catalogs. For more information, see Protect accidental machine deletion.

November 2021

New and enhanced features

Annotate an image when updating machines. In the Full Configuration management interface, you can now annotate an image by adding a note for it when updating an MCS-created catalog. Each time you update the catalog, a note-related entry is created whether you add a note. If you update the catalog without adding a note, the entry appears as null (-). To view note history for the image, select the catalog, click **Template Properties** in the lower pane, and then click **View note history**. For more information, see Update a catalog.

Multi-type licensing support. The Full Configuration management interface now supports multi-type licensing, letting you specify which license entitlement you want your site (your deployment of a Citrix Virtual Apps and Desktops service product) or a delivery group to use.

- At the site level, you determine which license to use site wide when users launch an app or a desktop on their devices. The selected license applies to all delivery groups, except those configured with a different license.
- At a delivery group level, you determine which license you want the delivery group to use, enjoying the multi-type licensing flexibility and benefits.

For more information, see Licenses.

Support for displaying Azure Marketplace purchase plan information. In the Full Configuration management interface, when creating a machine catalog, you can now view purchase plan information for master images originated from Azure Marketplace images.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

October 2021

New and enhanced features

Ability to update persistent MCS catalogs. We introduced the **Update Machines** option for persistent MCS catalogs in the Full Configuration management interface. The option lets you manage the image or template the catalog uses. When updating a persistent catalog, consider the following: Only machines you add to the catalog later are created using the new image or template. We do not roll out the update to existing machines in the catalog. For more information, see Update a catalog.

Option to provision VMs on an Azure dedicated host. We added an option, **Use a host group**, to the **Machine Catalog Setup > Master Image** page of the Full Configuration management interface. The option lets you specify which host group you want to use when provisioning VMs in Azure environments. For more information, see Create a machine catalog using an Azure Resource Manager image.

Improve performance by preserving a provisioned VM when power cycling. We added a setting, **Retain VMs across power cycles**, to the **Machine Catalog Setup > Disk Settings** page of the Full Configuration management interface. The setting lets you preserve a provisioned VM when power cycling in Azure environments. For more information, see MCS storage optimization. Alternatively, you can configure the feature by using PowerShell. For more information, see Preserving a provisioned virtual machine when power cycling.

Bind a machine catalog to a Workspace Environment Management configuration set. When creating a machine catalog, you can now bind it to a Workspace Environment Management configuration set. Doing so lets you use Workspace Environment Management service to deliver the best possible workspace experience to your users. You can also choose to bind the catalog after you create the catalog. For more information, see Create machine catalogs and Manage machine catalogs.

September 2021

New and enhanced features

Add informative description for image updates. You can now add informative descriptions about changes related to image updates for machine catalogs. This functionality is useful for administrators who want to add descriptive labels when updating an image used by a catalog, for example, *Office 365 installed*. Using PowerShell commands, you can create and view these messages. For details, see Adding descriptions to an image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure VMware Solution (AVS) integration. Citrix Virtual Apps and Desktops service supports AVS, the Azure VMware Solution. AVS provides cloud infrastructure containing vSphere clusters created by Azure. Leverage the Citrix Virtual Apps and Desktops service to use AVS for provisioning your VDA workload in the same way that you would using vSphere in on-premises environments. For more information, see Azure VMware Solution Integration.

Same resource group for multiple catalogs. You can now use the same resource group for updating and creating catalogs in Citrix Virtual Apps and Desktops service. This process:

- applies to any resource group that contains one or more machine catalogs.
- supports resource groups that are not created by Machine Creation Services.
- creates the VM and associated resources.
- deletes resources in the resource group when the VM or the catalog is removed.

For more information, see Azure Resource groups.

Retrieve information for Azure VMs, snapshots, OS disk, and gallery image definition. You can display information for an Azure VM, OS disk, snapshot, and gallery image definition. This information is displayed for resources on the master image when a machine catalog is assigned. Use this functionality to view and select either a Linux or Windows image. For more information, see Retrieve information for Azure VMs, snapshots, OS disk, and gallery image definition.

New update for Automated Configuration. Automated Configuration has been updated to a new version with features including:

- Machines Creation Services (MCS) support - Automated Configuration now supports MCS catalogs. For more information, see Understanding migrating Machine Creation Services provisioned catalogs.

Other updates to Automated Configuration include:

- Enhanced Zone support by pre-populating the ZoneMapping.yml file with the names of on-premises zones during export and cloud Resource Locations when backing up.
- StoreFront has been made a top level manageable component. Prior to this, StoreFront was managed as part of Delivery Groups. This separation better facilitates site merging.
- Changed `AddMachinesOnly` to `MergeMachines` to match the pattern for current and new merge options.
- Added the use of the SecurityClient.csv file to import the ClientId and Secret when creating and updating the CustomerInfo.yml when using the support cmdlets.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Added User Zone Preferences migration.
- Fixed support for the Japanese Control Plane.
- Other fixes and improvements.

Download Automated Configuration at Citrix Downloads. For more information on Automated Configuration, see Migrate configuration to Citrix Cloud.

More scheduling options available with restart schedules. The Full Configuration management interface now provides you with additional options to control when scheduled restarts occur. In addition to the daily recurring restart schedules, you can now set weekly and monthly recurrence patterns. For more information, see Create a restart schedule.

Preserve custom columns that degrade performance. Previously, on the **Search** node of the Full Configuration management interface, custom columns that degraded performance disappeared after you refreshed the browser window or signed out of the console and then signed in. You can now control whether to preserve those custom columns. For more information, see Use Search in the Full Configuration management interface.

Use the Automated Configuration tool to back up and restore. We added a node, **Backup and Restore**, to the Full Configuration management interface. That node aggregates all resources related to the Automated Configuration tool, including information about:

- Scheduling automated backups of your Citrix Virtual Apps and Desktops configuration using a single command
- Restoring from a previous backup if necessary
- Performing backups and restores granularly
- Other use cases supported

For more information, see the Automated Configuration documentation.

Support for non-domain-joined catalogs. We added an identity type, **Non-domain-joined**, to the **Machine Catalog Setup > Machine Identities** page of the Full Configuration management interface. With that identity type, you can use MCS to create machines that are not joined to any domain. For more information, see Create machine catalogs.

Support for using a machine profile. We added an option, **Use a machine profile**, to the **Machine Catalog Setup > Master Image** page of the Full Configuration management interface. The option lets you specify which machine profile you want the VMs to inherit configurations from

© 1997–2026 Citrix Systems, Inc. All rights reserved.

when creating VMs in Azure environments. The VMs in the catalog can then inherit configurations from the selected machine profile. Examples of configurations include:

- Accelerated networking
- Boot diagnostics
- Host disk caching (relating to OS and MCSIO disks)
- Machine size (unless otherwise specified)
- Tags placed on the VM

For more information, see Create a machine catalog using an Azure Resource Manager image.

Support for Windows Server 2022. Requires minimum VDA 2106.

August 2021

New and enhanced features

Extend the number of sortable items from 500 to 5,000. On the **Search** node of the Full Configuration management interface, you can now sort up to 5,000 items by any column header. When the number of items exceeds 5,000, use filters to reduce the number of items to 5,000 or fewer to enable sorting. For more information, see Use Search in the Full Configuration management interface.

Support for additional Azure storage types. You can now select different storage types for virtual machines in Azure environments using MCS. For details, see Storage types.

Support for selecting the storage type for write-back cache disks. In the Full Configuration management interface, when creating an MCS catalog, you can now select the storage type for the write-back cache disk. Available storage types include: Premium SSD, Standard SSD, and Standard HDD. For more information, see Create machine catalogs.

Shut down suspended machines. In the **Manage > Full Configuration** interface, we added an option, **When no reconnection in (minutes)**, to the **Load-based Settings** page of the Manage Autoscale user interface for single-session OS delivery groups. The option becomes available after you select **Suspend**, letting you specify when to shut down the suspended machines. Suspended machines remain available to disconnected users when they reconnect but are not available for new users. Shutting the machines down makes them available again to handle all workloads. For more information, see Autoscale.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Extended support for using CSV files to bulk add machines to a catalog. In the **Manage > Full Configuration** interface, you can now use a CSV file to bulk add machines already in your data center to a catalog where those machines are power managed. For more information, see Create machine catalogs and Manage machine catalogs.

July 2021

New and enhanced features

Configuration logging. The **Logging** user interface has changed in **Manage > Full Configuration**. The following three tabs comprise the interface:

- **Events** (formerly, configuration logging). This tab lets you track configuration changes and administrative activities.
- **Tasks**. This tab lets you view tasks related to machine catalog operations.
- **APIs**. This tab lets you view REST API requests made during a certain time period.

For more information, see Configuration logging.

Autoscale now provides you with dynamic session timeout options. You can configure disconnected and idle session timeouts for your peak and off-peak usage times to achieve faster machine draining and cost savings. For more information, see Dynamic session timeouts.

Support for Google Cloud Platform (GCP) Customer Managed Encryption Keys (CMEK). You can now use Google's CMEK with MCS catalogs. CMEK provides greater control over keys used to encrypt data within a Google Cloud project. For more information, see Customer-managed encryption keys (CMEK). To configure this feature, see Using Customer Managed Encryption Keys (CMEK). The feature is available on the **Machine Catalog Setup > Disk Settings** page of the **Manage > Full Configuration** interface.

NOTE:

This feature is available as a preview.

Updates to the Manage tab. We have updated options in the menu of the **Manage** tab:

- **Full Configuration**: Previously, this option took you to the legacy console. It now takes you to the new, web-based console (Web Studio). The web-based console has full parity with the legacy console and includes several enhancements. We recommend that you start using it now.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Legacy Configuration**: This option takes you to the legacy console, which is scheduled for removal in September 2021. After that, **Full Configuration** will be the only interface that offers access to the full range of configuration and management actions.

Web Studio now supports choosing a power management connection for a Remote PC Access catalog. Previously, you were able to use Studio to create a Wake on LAN host connection to your resource location (selecting **Remote PC Wake on LAN** as the connection type). However, PowerShell was your only choice to associate that connection with a Remote PC Access catalog. You can now use Studio to achieve that. For more information, see Configure Wake on LAN in the Full Configuration interface.

June 2021

New and enhanced features

Access Azure Shared Image Gallery images. When creating a machine catalog, you can now access images from the Azure Shared Image Gallery on the Master Image screen. For details, see Access images from Azure Shared Image Gallery.

Support shielded virtual machines on Google Cloud Platform (GCP). You can provision shielded virtual machines on GCP. A shielded virtual machine is hardened by a set of security controls that provide verifiable integrity of your Compute Engine instances, using advanced platform security capabilities like secure boot, a virtual trusted platform module, UEFI firmware and integrity monitoring. For more information, see Shield VMs.

Enforce either HTTPS or HTTP. Use registry settings to enforce HTTPS or HTTP traffic through the XML service.

Always use standard SSD for an identity disk to reduce cost in Azure environments. Machine catalogs use the standard SSD storage type for identity disks. Azure standard SSDs are a cost-effective storage option optimized for workloads that need consistent performance at lower IOPS levels. For more information about storage types, see Azure Resource Manager master image.

NOTE:

For more information about Azure managed disk pricing, see Managed Disks pricing.

New feature available in Web Studio. The following features are now available in the web-based console:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Studio now supports authenticating to Azure to create a service principal**. You can now establish a host connection to Azure by authenticating to Azure to create a service principal. This support eliminates the need to manually create a service principal in your Azure subscription before creating a connection in Studio. For more information, see Microsoft Azure Resource Manager virtualization environments.
- **Studio now supports cloning of existing machine catalogs**. This feature enables you to clone an existing machine catalog to use as a template for a new one, eliminating the need to create a similar catalog from scratch. When cloning a catalog, you cannot change settings associated with operating system and machine management. The cloned catalog inherits those settings from the original. For more information, see Clone a catalog.
- **A new node called Settings now available in the Studio navigation pane**. The **Settings** node lets you configure settings that apply to the entire site (your deployment of a Citrix Virtual Apps and Desktops service product). The following settings are available:
  - **Load balance multi-session catalogs**. Select the load balancing option that meets your needs. This setting applies to all your catalogs. Previously, you accessed this feature by clicking the gear icon in the upper right corner of the console. For more information, see Load balance machines.
- **Enhanced search experience in Studio**. This release enhances your Studio search experience. When you use filters to perform an advanced search, the Add filters window appears in the foreground, leaving the background view unchanged. For more information, see Use Search in the Full Configuration management interface.
- **Ability to suspend and resume Google Cloud VMs in MCS**. You can now suspend and resume Google Cloud VMs in MCS as you would any VM. For details, see Manage delivery groups. To enable this ability, set the `compute.instances.suspend` and `compute.instances.resume` permissions in the Google Cloud service account. The Compute Admin role comes with these permissions.

  In Citrix Virtual Apps and Desktops, you can also use the `New-BrokerHostingPowerAction` PowerShell command to suspend and resume the VMs. For details, see New-Brokerhostingpoweraction.

  Google Cloud enforces some limitations on the type and configuration of instances that can be suspended. For additional information, refer to Suspending and resuming an instance on the Google Cloud site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 2021

New and enhanced features

Session reconnection after disconnect from machine in maintenance mode. Previously, when pooled (random) single-session desktop (VDI) users were disconnected from a machine in maintenance mode, session reconnection was not allowed to any machine in the pool. Multi-session and static single-session machines always allowed session reconnection in that circumstance.

Now, using PowerShell, you can control at the delivery group level whether session reconnection is allowed after a disconnect occurs on a machine in maintenance mode. This applies to all VDAs in the group (single-session and multi-session).

For details, see Control session reconnection when disconnected from machine in maintenance mode.

Application probing and Desktop probing support in all Citrix Virtual Apps and Desktops Service editions. In addition to the existing **Premium** edition support, Application probing and Desktop probing are now available in **Citrix Virtual Apps Advanced Service** and **Citrix Virtual Apps and Desktops Advanced Service** editions.

New feature available in Web Studio. The following feature is now available in the web-based console:

- **Studio now supports selecting Azure Availability Zones**. Previously, PowerShell was your only choice to provision machines into a specific Availability Zone in Azure environments. When using Studio to create a machine catalog, you can now select one or more Availability Zones into which you want to provision machines. If no zones are specified, Machine Creation Services (MCS) lets Azure place the machines within the region. If more than one zone is specified, MCS randomly distributes the machines across them. For more information, see Provision machines into specified availability zones.

Azure emphemeral disk. Citrix Virtual Apps and Desktops service supports Azure ephemeral disk. An ephemeral disk allows you to repurpose the cache disk to store the OS disk for an Azure-enabled virtual machine. This functionality is useful for Azure environments that require a higher performant SSD disk over a standard HDD disk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Persistent catalogs do not support ephemeral OS disks. Also, when using this feature, consider that the extra performant disk incurs an extra cost. It's beneficial to reuse the cache disk to store the OS disk instead of paying for an extra managed disk.

Ephemeral OS disks require that your provisioning scheme use managed disks and a Shared Image Gallery. For more information, see Azure ephemeral disks.

Improved performance for MCS managed VDAs on Azure. The Citrix Virtual Apps and Desktops service improves performance for VDAs managed with Machine Creation Services (MCS) on Azure. This enhancement changes the default values for *Absolute Simultaneous actions* for the hosting connection to 500, and *Maximum new actions per minute* for the hosting connection to 2,000. No manual configuration tasks are required to take advantage of this enhancement. For details, see Azure throttling.

New features available in Cloud Health Check. Cloud Health Check has been updated to a new version with features including:

- **Automatically discovering VDA machines**. Cloud Health Check can now automatically discover and retrieve VDAs from your Citrix Virtual Apps and Desktops service deployments. For more information, see Retrieve VDA machines.
- **Scheduling health checks**. Cloud Health Check now lets you set up schedules for performing periodic health checks. For more information, see Cloud Health Check scheduler.
- **Cloud Health Check version information**. You can now check which version of Cloud Health Check you are using. To view version information, click the gear icon in the upper right corner of the Cloud Health Check main window.
- **Automatic fix**. Cloud Health Check now supports automatically detecting and fixing certain issues identified on machines where it is running. For more information, see Automatic fix.

  NOTE:

  Automatic fix is available as a preview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 2021

New and enhanced features

Retreive dynamic instances using AWS API. The Citrix Virtual Apps and Desktops service now queries AWS to retrieve instance types dynamically. This functionality removes the need to create a custom `InstanceTypes.xml` file for those customers wishing to use machine sizes beyond those defined in Citrix Virtual Apps and Desktops service. This information was previously supplied by the `InstanceTypes.xml` file. To facilitate this dynamic access to the available AWS instance types, users must update the permissions on their service principals to include `ec2:DescribeInstanceTypes` permissions. To support backward compatibility for customers who choose not to update their service principal permissions, the AWS instance types listed in the `InstanceTypes.xml` are used. This process generates a warning message to the MCS CDF log.

NOTE:

Citrix Studio does not display the warning message contained in the CDF log.

For more information about permissions, see Defining IAM permissions and About AWS permissions.

New feature available in Web Studio. The following feature is now available in the web-based console:

- **Studio now displays date and time of your time zone**. Previously, Studio displayed only date and time based on the system clock and time zone. Studio now supports displaying date and time local to your time zone when you hover the mouse pointer over an event item. The time is expressed in UTC.

MCS I/O support for Azure VMs without temporary storage. MCS I/O now supports machine catalog creation for VMs that do not have temporary disks or attached storage. With this support:

- The snapshot (managed disk) is retrieved from the source VM *without* temporary storage. The VMs in the machine catalog have no temporary storage.
- The snapshot (managed disk) is retrieved from the source VM *with* temporary storage. The VMs in the machine catalog have temporary storage.

For more information, see Machine Creation Services (MCS) storage optimization

New feature available in Web Studio. The following feature is now available in the web-based console:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Force log off**. Autoscale now lets you log off sessions existing on machines by force when the established grace period is reached, making the machine eligible for shutdown. Doing that enables Autoscale to power off machines much faster, thus reducing costs. You can send notifications to users before they are logged off. For more information, see Autoscale.

New update for Automated Configuration. Automated Configuration has been updated to a new version with features including:

- **Merging multiple sites** – you can merge multiple sites into a single site while avoiding name collisions using prefixes and suffixes. For more information, see Merging multiple sites into a single site.
- **Site activation** – you can select whether your on-premises or cloud deployment controls resources such as reboot schedules and power schemes. For more information, see Activating sites.

Other updates to Automated Configuration include:

- The ability to migrate administrator roles and scopes.
- A `Quiet` parameter for select cmdlets to suppress console logging.
- A `SecurityFileFolder` parameter to allow placing of the CvadAcSecurity.yml file in a secure network file share that requires authentication.
- The ability to filter by machine name in machine catalogs and delivery groups.
- Improvements to component selection parameters to use the switch parameter method, eliminating the need to add a `$true` after the component name.
- A new cmdlet (`New-CvadAcZipInfoForSupport`) to zip all your log files to send to Citrix for support.

Download Automated Configuration at Citrix Downloads. For more information on Automated Configuration, see Migrating to cloud.

Preserve GCP instances across power cycles. Non-persistent Google Cloud Platform (GCP) instances are no longer deleted when powering off. Instead, the instances are preserved across power cycles. When a non-persistent instance is powered off, the OS disk is detached and deleted. When the instance is powered on, the OS disk is recreated from the base disk, and attached to the existing instance.

Support for Azure Gen2 images. You can now provision a Gen2 VM catalog by using either a Gen2 snapshot or a Gen 2 managed disk to improve boot time performance. For more information,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

see Create machine catalogs. The following operating systems are supported for Azure Gen2 images:

- Windows Server 2019, 2016, 2012 and 2012 R2
- Windows 10

NOTE:

Creating a Gen2 machine catalog using a Gen1 snapshot, or managed disk, is not supported. Similarly, creating a Gen1 machine catalog using a Gen2 snapshot, or managed disk, is also not supported. For more information, see Support for generation 2 VMs on Azure.

Disabling table storage accounts. Machine Creation Services (MCS) no longer creates table storage accounts for catalogs that use managed disks when provisioning VDAs on Azure. For more information, see Azure table storage.

Eliminating locks in storage accounts. When creating a catalog in Azure using a managed disk, a storage account is no longer created. Storage accounts created for existing catalogs remain unchanged. This change is applicable for managed disks only. For unmanaged disks, there is no change in the existing behavior. Machine Creation Services (MCS) continues creating storage accounts and locks.

New features available in Web Studio. The following features are now available in the web-based console:

- **Use a customer-managed encryption key to encrypt data on machines**. Studio now adds a setting called **Customer-managed encryption key** to the **Machine Catalog Setup > Disk Settings** page. The setting lets you choose whether to encrypt data on the machines to be provisioned in the catalog. For more information, see Customer-managed encryption key.
- **Studio now supports restricting Autoscale to tagged machines**. Previously, you had to use PowerShell to restrict Autoscale to certain machines in a delivery group. You can now also use Studio. For more information, see Restrict Autoscale to certain machines in a delivery group.

March 2021

New and enhanced features

Azure dedicated hosts. Azure dedicated hosts allow you to provision virtual machines on hardware dedicated to a single customer. While using a dedicated host, Azure ensures that your virtual machines would be the only machines running on that host. This provides more control and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

visibility to customers thereby ensuring they meet their regulatory or internal security requirements. A pre-configured Azure host group, in the region of the hosting unit, is required when using the `HostGroupId` parameter. Also, Azure auto-placement is required. For more information, see Azure dedicated hosts.

TIP:

When using Azure dedicated hosts, selecting the **Azure Availability Zone** has no effect. The virtual machine is placed by the Azure auto-placement process.

Support for Azure server side encryption. Citrix Virtual Apps and Desktops service supports customer-managed encryption keys for Azure managed disks. With this support you can manage your organizational and compliance requirements by encrypting the managed disks of your machine catalog using your own encryption key. For more information, see Azure server side encryption.

Provision machines into specified availability zones on Azure. You can now provision machines into a specific availability zone in Azure environments. With this functionality:

- You can specify one or multiple Availability Zones on Azure. Machines are nominally equally distributed across all provided zones if more than one zone is provided.
- The virtual machine and the corresponding disk are placed in the specified zone (or zones).
- You can browse Availability Zones for a given service offering or region. Valid Availability Zones are displayed using PowerShell commands. View service offering inventory items using `Get-Item`.

For more information, see Provision machines into specified availability zones on Azure.

New features available in Web Studio. The following features are now available in the web-based console:

- **Studio now supports associating apps with custom icons**. Previously, you had to use PowerShell to add custom icons for use with published applications. You can now also use Studio to do that. For more information, see Manage application groups.
- **Studio now supports applying tags to machine catalogs**. Previously, you might use Studio to create or delete tags for use with a catalog. However, you had to use PowerShell to apply tags to the catalog. You can now also use Studio to apply or remove a tag to or from a catalog as you do with delivery groups. For more information, see Apply tags to machine catalogs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Studio now supports switching between "horizontal load balancing" and "vertical load balancing" modes**. Previously, PowerShell was your only choice to switch between horizontal and vertical load balancing modes. Studio now gives you more flexibility to control how to load balance multi-session OS machines. For more information, see Load balance machines.
- **Studio now supports including machines in maintenance mode in restart schedules**. Previously, PowerShell was your only choice to configure scheduled restarts for machines in maintenance mode. You can now also use Studio to control whether to include those machines in a restart schedule. For more information, see Create a restart schedule.
- **Studio now supports configuring Wake on LAN for Remote PC Access**. Previously, you had to use PowerShell to configure Wake on LAN for Remote PC Access. You can now also use Studio to configure the feature. For more information, see Configure Wake on LAN.
- **Studio now supports applying AWS instance properties and tagging operational resources**. When creating a catalog to provision machines in AWS by using MCS, you can specify whether to apply the IAM role and tag properties to those machines. You can also specify whether to apply machine tags to operational resources. You have the following two options:

  - **Apply machine template properties to virtual machines**
  - **Apply machine tags to operational resources**

  For more information, see Applying AWS instance properties and tagging operational resources.

Azure Shared Image Gallery. Citrix Virtual Apps and Desktops service supports Azure Shared Image Gallery as a published image repository for MCS provisioned machines in Azure. Administrators have the option of storing an image in the gallery to accelerate the creation and hydration of OS disks. This process improves the boot and application launch times for non-persistent VMs. For details about this feature, see Azure shared image gallery.

NOTE:

Shared Image Gallery functionality is compatible with managed disks. It is not available for legacy machine catalogs.

Storage buckets created in same Google Cloud Platform region as the machine catalog. In previous releases, MCS created temporary storage buckets during provisioning as part of the disk upload process. These buckets spanned multiple regions, which Google defines as a large geographic area containing two or more geographic places. These temporary buckets resided in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the United States geographic location, no matter where the catalog was provisioned. MCS now creates storage buckets in the same region where you provision your catalogs. Storage buckets are no longer temporary; they remain in your Google Cloud Platform project after you complete the provisioning process. Future provisioning operations use the existing storage bucket, if one exists in that region. A new storage bucket is created if one does not exist in the specified region.

February 2021

New and enhanced features

Support for Azure Gen2 images. You can now provision managed disks using Gen2 VMs in Azure environments to improve boot time performance. The following operating systems are supported:

- Windows Server 2019, 2016, 2012 and 2012 R2
- Windows 10

NOTE:

With this support, only a subset of VMs is supported. For example, some VMs can be both Gen1 and Gen2 types, while other VMs can only be Gen1. For more information, see Support for generation 2 VMs on Azure.

Machine restart schedules. Citrix Studio now adds an option called **Restart all machines after draining sessions** to the **Restart duration** menu. The option lets you choose whether to restart all machines after draining all sessions. When the restart time is reached, machines are put into the drain state and restarted when all sessions are logged off. For more information, see Create a restart schedule.

New features available in Web Studio. The following features are now available in the web-based console:

- **Studio now supports using CSV files to bulk add machines to a catalog**. This feature enables you to use a CSV file to:
  - Bulk add machines to a multi-session or single-session OS catalog where machines are not power managed through Studio.
  - Bulk add machines to a Remote PC Access catalog. Previously, you had to choose OUs to bulk add machines to a Remote PC Access catalog. Doing that, however, is not easy in scenarios with OU structure restrictions. The feature gives you more flexibility to bulk add

© 1997–2026 Citrix Systems, Inc. All rights reserved.

machines. You can add only machines (for use with user auto-assignments) or add machines along with user assignments.

For more information, see Create machine catalogs and Manage machine catalogs.

- **Extended support for Citrix Managed Azure.** Citrix Managed Azure is now available in the following Citrix Virtual Apps and Desktops service editions: Standard for Azure, Advanced, Premium, and Workspace Premium Plus.
- **Support for placing master images in Azure Shared Image Gallery**. Studio now provides you an option to place master images in Azure Shared Image Gallery (SIG). SIG is a repository for managing and sharing images. It lets you make your images available throughout your organization. We recommend that you store a master image in SIG when creating large non-persistent machine catalogs because doing that enables faster reset of VDA OS disks. For more information, see Microsoft Azure Resource Manager virtualization environments.
- **Retain system disk for MCS machine catalogs in Azure**. Studio now lets you control whether to retain system disks for VDAs during power cycles. Ordinarily, the system disk is deleted on shutdown and recreated on startup. This ensures that the disk is always in a clean state but results in longer VM restart times. If system writes are redirected to the cache and written back to the cache disk, the system disk remains unchanged. To avoid unnecessary disk recreation, use the **Retain system disk during power cycles** option, available on the **Machine Catalog Setup > Disk Settings** page. Enabling the option reduces VM restart times but increases your storage costs. The option can be useful in scenarios where an environment contains workloads with sensitive restart times. For more information, see MCS storage optimization.
- **Studio now supports creating MCS machine catalogs with persistent write-back cache disk**. Previously, PowerShell was your only choice to create a catalog with persistent write-back cache disk. You can now use Studio to control whether the write-back cache disk persists for the provisioned VMs in Azure when you are creating a catalog. If disabled, the write-back cache disk is deleted during each power cycle to save storage costs, causing any data redirected to the disk to be lost. To retain the data, enable the **Use persistent write-back cache disk** option, available on the **Machine Catalog Setup > Disk Settings** page. For more information, see MCS storage optimization.

Support for App protection for Citrix Virtual Apps and Desktops Service with StoreFront. For more information, see the App protection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 2021

New features available in Web Studio. The following features are now available in the web-based console:

- **Studio now supports associating apps with custom icons**. Previously, you had to use PowerShell to add custom icons for use with published applications. You can now also use Studio to do that. For more information, see Manage application groups.
- **Studio now supports applying tags to machine catalogs**. Previously, you might use Studio to create or delete tags for use with a catalog. However, you had to use PowerShell to apply tags to the catalog. You can now also use Studio to apply or remove a tag to or from a catalog as you do with delivery groups. For more information, see Apply tags to machine catalogs.
- **Studio now supports switching between "horizontal load balancing" and "vertical load balancing" modes**. Previously, PowerShell was your only choice to switch between horizontal and vertical load balancing modes. Studio now gives you more flexibility to control how to load balance multi-session OS machines. For more information, see Load balance machines.
- **Studio now supports including machines in maintenance mode in restart schedules**. Previously, PowerShell was your only choice to configure scheduled restarts for machines in maintenance mode. You can now also use Studio to control whether to include those machines in a restart schedule. For more information, see Create a restart schedule.
- **Studio now supports configuring Wake on LAN for Remote PC Access**. Previously, you had to use PowerShell to configure Wake on LAN for Remote PC Access. You can now also use Studio to configure the feature. For more information, see Configure Wake on LAN.
- **Studio now supports applying AWS instance properties and tagging operational resources**. When creating a catalog to provision machines in AWS by using MCS, you can specify whether to apply the IAM role and tag properties to those machines. You can also specify whether to apply machine tags to operational resources. You have the following two options:

  - **Apply machine template properties to virtual machines**
  - **Apply machine tags to operational resources**

  For more information, see Applying AWS instance properties and tagging operational resources.
- **AWS dedicated host**. Citrix Studio now adds an option called **Use dedicated host** to the **Machine Catalog Setup > Security** page. This setting is suitable for deployments with licensing restrictions or security requirements that need your use of a dedicated host. With a dedicated host, you own an entire physical host and are billed on an hourly basis. Owning that

© 1997–2026 Citrix Systems, Inc. All rights reserved.

host lets you spin up as many EC2 instances as that host permits, without more charges. For more information, see AWS tenancy.

- **Studio now supports running a restart schedule immediately**. Studio now lets you run a restart schedule immediately to restart all applicable machines in the schedule. For more information, see Immediately run a restart schedule.
- **Autoscale**. Autoscale provides the following new features and enhancements:
  - **Studio now supports displaying machines in drain state**. Previously, PowerShell was your only choice to identify machines in drain state. You can now use Studio to identify machines that are in drain state. For more information, see Display machines in drain state.
  - **Studio now supports defining peak times at a granular level of 30 minutes for VDI delivery groups**. Previously, you had to use PowerShell to define the peak times for the days included in a schedule at a granular level of 30 minutes for VDI delivery groups. You can now also use Studio to do that. This support enables you to set the minimum number of machines running in a VDI Delivery Group separately for each half hour of the day.

Azure Shared Image Gallery. Citrix Virtual Apps and Desktops service supports Azure Shared Image Gallery as a published image repository for MCS provisioned machines in Azure. Administrators have the option of storing an image in the gallery to accelerate the creation and hydration of OS disks from the master image. This process improves the boot and application launch times for non-persistent VMs.

The gallery contains the following three elements:

- Gallery. Images are stored here. MCS creates one gallery for each machine catalog.
- Gallery Image Definition. This definition includes information (operating system type and state, Azure region) about the master image. MCS creates one image definition for each master image created for the catalog.
- Gallery Image Version. Each image in a Shared Image Gallery can have multiple versions, and each version can have multiple replicas in different regions. Each replica is a full copy of the master image. Citrix Virtual Apps and Desktops service always creates one Standard_LRS image version (version 1.0.0) for each image with the appropriate number of replicas in the catalog's region. This configuration is based on the number of machines in the catalog, the configured replica ratio, and the configured replica maximum.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

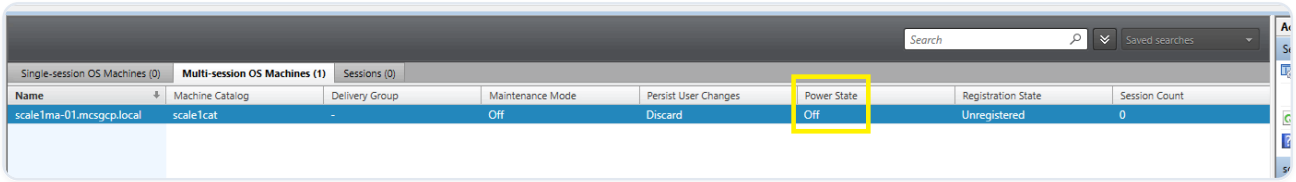
Shared Image Gallery functionality only works with managed disks. It is not available for legacy machine catalogs.

For details about this feature, see Configure shared image gallery.

Storage buckets created in same Google Cloud Platform region as the machine catalog. In previous releases, MCS created temporary storage buckets during provisioning as part of the disk upload process. These buckets spanned multiple regions, which Google defines as a large geographic area containing two or more geographic places. These temporary buckets resided in the United States geographic location, no matter where the catalog was provisioned. MCS now creates storage buckets in the same region where you provision your catalogs. Storage buckets are no longer temporary; they remain in your Google Cloud Platform project after you complete the provisioning process. Future provisioning operations use the existing storage bucket. If one exists in that region, or a new storage bucket is created if one does not exist in the specified region.

PowerShell option that sets default to re-use pooled VDAs during an outage. A new PowerShell command option (`-DefaultReuseMachinesWithoutShutdownInOutage`) extends the ability to reuse pooled desktop VDAs that haven't been shut down during an outage, by default. See Application and desktop support.

Google Cloud Platform on-demand provisioning. Citrix Virtual Apps and Desktops service updates how the Google Cloud Platform (GCP) provisions machine catalogs. When creating a machine catalog, the corresponding machine instance is not created in GCP and the power state is set to **OFF**. Machines are not provisioned at catalog creation time but rather the first time the machines are powered on. For example, after you create a catalog, the VM power state is set to **Off**:



December 2020

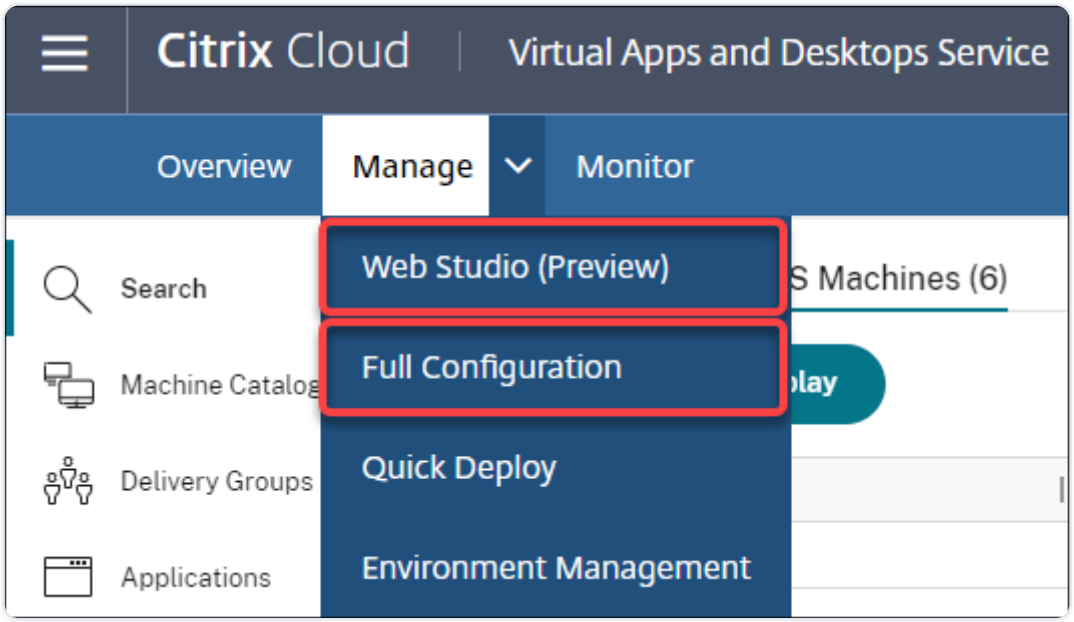
New and enhanced features

Web Studio is available as a preview. A new, web-based console is now available. We are in the process of migrating the full set of Studio functionalities from the legacy console to the new, web-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

based console. The web-based console generally responds faster than the legacy console. By default, you automatically log on to the web-based console. You can easily switch between the web-based console and the legacy console from within the **Manage** tab to perform your configuration or site management tasks. Click the down arrow next to **Manage** and select an option:

- **Web Studio (Preview)**. Takes you to the new, web-based console.
- **Full Configuration**. Takes you to the legacy console.



The following features are available only in the web-based console:

- **Standard SSD disk type support for Azure**. Studio now adds support for standard SSD disk type. Azure standard SSDs are a cost-effective storage option optimized for workloads that need consistent performance at lower IOPS levels. For more information, see Create a machine catalog using an Azure Resource Manager master image.
- **Studio now supports configuring the power-off delay for static VDI delivery groups**. Previously, you might configure the power-off delay for static VDI delivery groups only through the PowerShell SDK. Studio now lets you configure the power-off delay in the Autoscale user interface for static VDI delivery groups. For more information, see Autoscale.

October 2020

New and enhanced features

Dismiss multiple hypervisor alerts. Citrix Monitor now supports automatic dismissal of hypervisor alerts older than a day. For more information, see Hypervisor Alerts Monitoring.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remove external IP address. An external IP address on a temporary virtual machine that is used to prepare a provisioned image in the Google Cloud Platform (GCP) is no longer required. This external IP address enables the temporary virtual machine to access the Google public API to complete the provisioning process.

Enable Private Google Access to permit the VM to access the Google public API directly from the subnet. For more information, see Enable Google Private access.

New model addresses how machine identities are managed. Machine identities used in machine catalogs have been managed and maintained using Active Directory. All machines created by MCS will now be joining Active Directory. The new Citrix Virtual Apps and Desktops service model addresses how machine identities are managed. This model allows the creation of machine catalogs using *workgroup*, or, non-domain joined machines.

TIP:

This functionality supports a new identity service, *FMA trust*, added to Citrix Cloud for non-domain joined machines.

MCS communicates with the new FMA trust service for identity management. Identity information is stored in the identity disk as a pair of GUID and private key pairs, instead of the domain SID and machine account password paradigm used by Active Directory. VDAs using non-domain joined machines use this GUID and private key combination for broker registration. For more information, see Configure support for non-domain joined catalogs.

Use direct upload for Azure managed disks. This release allows you to use direct upload when creating managed disks in an Azure environment. This functionality reduces costs associated with extra storage accounts. You no longer have to stage the VHD into a storage account before converting it to a managed disk. Also, direct upload eliminates the need to attach an empty managed disk to a virtual machine. Directly uploading to an Azure managed disk simplifies the workflow by enabling you to copy an on-premises VHD directly for use as a managed disk. Supported managed disks include Standard HDD, Standard SSD, and Premium SSD.

For more information on this feature, see the Microsoft Azure blog.

For more information about Azure managed disks, see the documentation page.

Single Resource Group in Azure. You can now create and use a single Azure resource group for updating and creating catalogs in Citrix Virtual Apps and Desktops. This enhancement applies to both the full scope and narrow scope service principals. The previous limit of 240 VMs per 800

© 1997–2026 Citrix Systems, Inc. All rights reserved.

managed disks per Azure Resource Group has been removed. There is no longer a limit on the number of virtual machines, managed disks, snapshots, and images per Azure Resource Group.

For more information, see Microsoft Azure Resource Manager virtualization environments.

September 2020

New and enhanced features

Quick Deploy. The new Quick Deploy feature replaces the earlier Azure Quick Deploy. The new feature offers a quick way to get started with the Citrix Virtual Apps and Desktops service using Microsoft Azure. You can use Quick Deploy to deliver desktops and apps, and configure Remote PC Access.

Session Administrator (built-in role). Citrix Studio now adds a new built-in role called **Session Administrator**. The role lets an administrator view delivery groups and manage their associated sessions and machines on the **Filters** page of the **Monitor** tab. With this feature, you can configure access permissions of existing administrators or administrators you invite in a way that aligns with their role in your organization. For more information about the built-in role, see Built-in roles and scopes. For information about how to assign the built-in role to an administrator, see Delegated administration and monitoring.

For a more granular level of control over access to the **Filters** page related to sessions and machines, create a custom role and select one of the following for the Director object: **View Filters page - Machines only**, **View Filters page - Sessions only**. For information about creating a custom role, see Create and manage roles.

Support for a new machine type. This release adds support for the NV v4 and the DA v4 series of AMD machines, when configuring Premium Disks for a machine catalog. For more information, see Create delivery groups.

August 2020

New and enhanced features

Limited access to the Remote PowerShell SDK during an outage. Previously, you might not use PowerShell commands during an outage. Now, Local Host Cache allows limited access to the Remote PowerShell SDK during an outage. See What is unavailable during an outage.

Support for two new Citrix Virtual Apps and Desktops service editions. Citrix Monitor now supports two new Citrix Virtual Apps and Desktops service editions, namely, **Citrix Virtual Apps**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Advanced service and **Citrix Virtual Apps and Desktops Advanced service**. For more information, see the Citrix Monitor Feature compatibility matrix.

Support for shared Virtual Private Cloud (VPC) in Google Cloud Platform. The Citrix Virtual Apps and Desktops service supports Shared VPC on Google Cloud Platform as a host resource. You can use Machine Creation Services (MCS) to provision machines in a Shared VPC and manage them using Citrix Studio. For information about Shared VPC, see Shared Virtual Private Cloud.

Zone selection support for Google Cloud Platform. The Citrix Virtual Apps and Desktops service supports zone selection on Google Cloud Platform. This feature allows administrators to specify one or multiple zones within a region for catalog creation.

For sole-tenant type VMs, zone selection provides administrators with the ability to place sole tenant nodes across zones of their choice. For non-sole tenant VMs, zone selection provides the ability to place VMs deterministically across zones of their choice thereby providing flexibility in designing the deployment. For configuration information, see Enable zone selection.

Also:

- Sole tenancy provides exclusive access to a sole tenant node, which is a physical compute engine server dedicated to hosting only your project's VMs. These nodes allow you to group your VMs together on the same hardware or separate your VMs from other project's VMs.
- Sole tenant nodes help you meet dedicated hardware requirements for Bring Your Own License (BYOL) scenarios. They also enable you to comply with network access control policy, security, and privacy requirements such as HIPAA.

NOTE:

Sole tenancy is the only route to using Windows 10 VDI deployments on Google Cloud. Server VDI also supports this method. A detailed description for sole tenancy can be found on the Google documentation site.

Improved boot performance for Azure system disks. This release supports improved boot performance for Citrix Cloud implementations using Azure when MCSIO is enabled. With this support, you can retain the system disk. This provides the following advantages:

- VMs and applications now boot and launch with performance similar to how the golden image is served.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Reduction in API quota consumption, deleting and creating the system disk, and state transition delay caused when you delete a VM.

For example, use the PowerShell `PersistOSDisk` custom property in the `New-ProvScheme` command to configure this feature.

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>'
```

For more configuration information, see Improve boot performance.

July 2020

New and enhanced features

Support for granular, role-based access to the Filters page. Citrix Studio now provides more granular control over access to the **Monitor > Filters** page when you create a custom role. Specifically, you can assign permissions to view any combination of **Machines**, **Sessions**, **Connections**, and **Application Instances** to a custom role. The following are four more options for the **Director** object in the **Create Role** window:

- View Filters page - Application Instances only
- View Filters page - Connections only
- View Filters page - Machines only
- View Filters page - Sessions only

For information about creating roles, see Create and manage roles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Power-off delay support for assigned VDI machines (PowerShell only). In earlier releases, the power-off delay applied only to unassigned machines. Starting with this release, the power-off delay applies to both assigned and unassigned machines. For more information, see How Autoscale power manages machines.

Support for Windows Client licenses. The Citrix Virtual Apps and Desktops service now supports using Windows Client licenses to provision VMs in Azure. To run Windows 10 VMs in Azure, verify that your volume licensing agreement with Microsoft qualifies for this usage. For more information, see Create a machine catalog using an Azure Resource Manager master image.

May 2020

New and enhanced features

Machine restart schedules. You can now indicate whether a restart schedule affects machines that are in maintenance mode. This feature is available only in PowerShell. For details, see Scheduled restarts for machines in maintenance mode.

Resource availability. You can now ensure resource availability during an outage without having to publish resources in every zone (resource location). For details, see Resource availability.

April 2020

New and enhanced features

Enhanced scheduling granularity for VDI Delivery Groups (PowerShell only). Autoscale now supports defining the peak times for the days included in a schedule at a granular level of 30 minutes. You can set the minimum number of machines running in a VDI Delivery Group separately for each half hour of the day. Also, Autoscale can now scale up or down the number of powered-on machines in VDI Delivery Groups on a half-hourly basis instead of on an hourly basis. For more information, see Broker PowerShell SDK commands.

MTU Discovery. The Citrix protocol Enlightened Data Transport (EDT) now has MTU Discovery capabilities. MTU Discovery allows EDT to automatically determine and set the payload size for the session. This feature enables the ICA session to adjust to networks with non-standard Maximum Transmission Unit (MTU) or Maximum Segment Size (MSS) requirements. The ability to adjust avoids packet fragmentation that might result in degraded performance or failure to establish an ICA session. This update requires a minimum of Citrix Workspace app 1911 for Windows. If using Citrix Gateway, the minimum Citrix ADC firmware version required is 13.0.52.24 or 12.1.56.22. For more information, see EDT MTU Discovery.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

March 2020

New and enhanced features

PVS target device metrics. Citrix Monitor now provides a PVS target device metrics panel on the Machine Details page. Use the panel to view the status of Provisioning target devices for single-session and multi-session OS machines. Several metrics for Network, Boot, and Cache are available on this panel. These metrics help you monitor and troubleshoot PVS target devices to ensure that they are up and running. For more information, see PVS target device metrics.

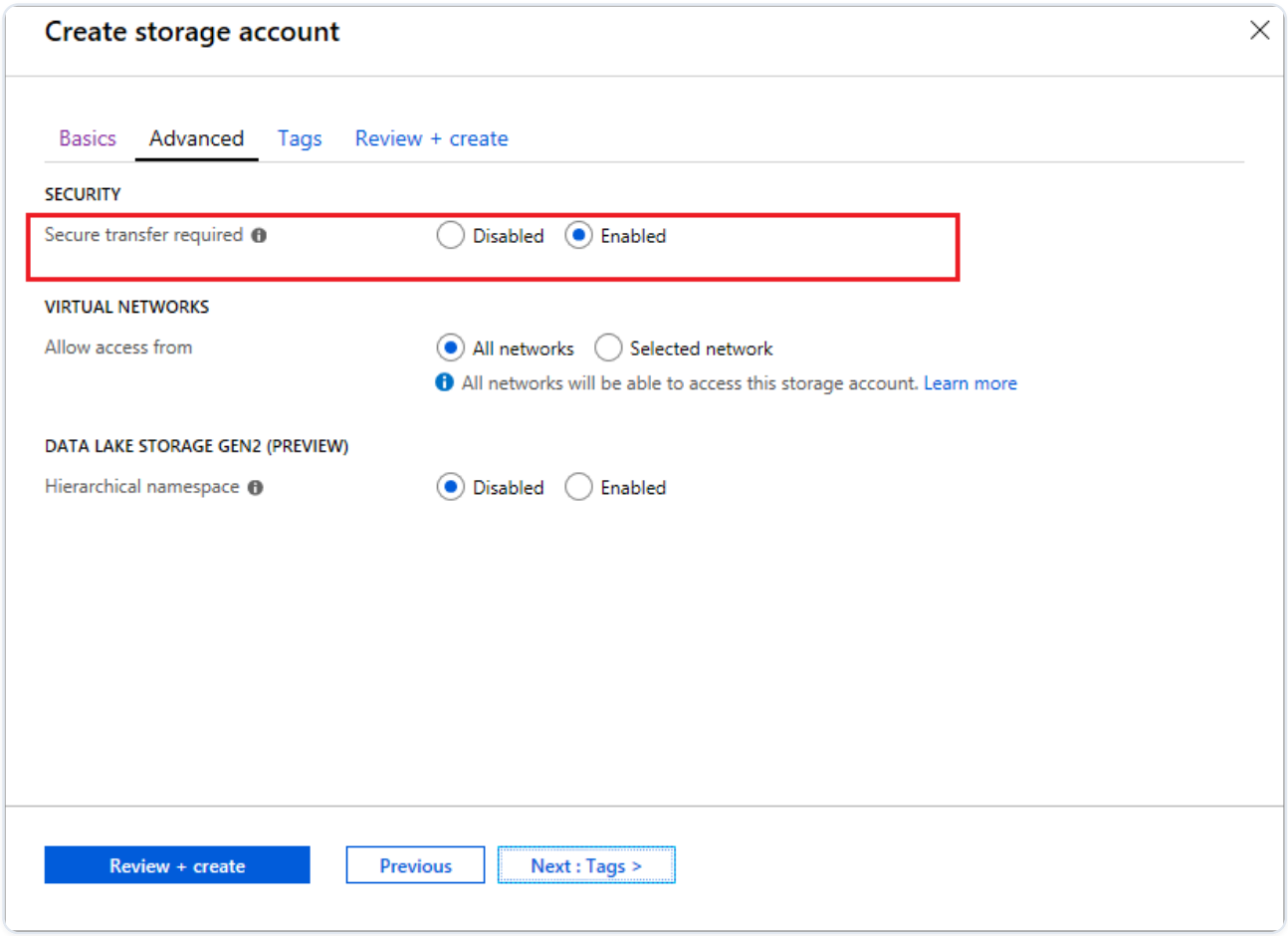
AWS instance property capturing. MCS now reads properties from the instance from which the AMI was taken and applies the IAM role and tags of the machine to the machines provisioned for a given catalog. When using this optional feature, the catalog creation process finds the selected AMI source instance, reading a limited set of properties. These properties are then stored in an AWS Launch Template, which is used to provision machines for that catalog. Any machine in the catalog inherits the captured instance properties. For more information, see AWS instance property capturing.

AWS operational resource tagging. This release introduces an option to tag resources created by Citrix components during provisioning. Each tag represents a label consisting of a customer-defined key and an optional value that improve your ability to manage, search for, and filter resources. For more information, see AWS operational resource tagging.

Secure transfer in Azure storage. Machine Creation Services (MCS) provides an enhancement for storage accounts created by MCS-provisioned catalogs in Azure Resource Manager environments. This enhancement automatically enables the secure transfer required property. This option enhances storage account security by only allowing requests to the account from secure connections. For more information, see Require secure transfer to ensure secure connections on the Microsoft site.

Enable the **Secure transfer required** property when creating a storage account in Azure:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Support for Azure SSD managed disks. Machine Creation Services (MCS) supports standard SSD managed disks for Azure virtual machines. This disk type provides consistent performance, and delivers better availability compared to HDD disks. For more information, see Standard SSD Disks for Azure Virtual machine workloads.

Use the PowerShell `StorageAccountType` custom property in the `New-ProvScheme` command or `Set-ProvScheme` command to configure this feature:

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /><Property
xsi:type=`"StringProperty`" Value=`"Windows_Server`" />
```

NOTE:

This feature is only available when using managed disks, that is, the custom property `UseManagedDisks` is set to **true**. For unmanaged disks only Standard HDD and Premium SSD are supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 2020

New and enhanced features

Language bar in Citrix Studio. Starting with this release, Citrix Studio provides a language bar to facilitate correct keyboard mapping.

- If the language of Citrix Cloud or the display language of your browser is set to **English** or **Japanese**, the language bar does not appear.
- If the language of Citrix Cloud or the display language of your browser is set to **German**, **Spanish**, or **French**, the language bar appears after you log on to Citrix Studio. There are two language options on the language bar list. Select an option that matches the topmost language of your browser.

  TIP:

  - Settings that you configure for the language bar might not take effect. In this case, log out and log back on.
  - You might fail to input certain symbols and localized characters by using the language bar. To resolve the issue, you need to configure the language of Citrix Cloud, the display language of your browser, and the local keyboard layout. For more information, see Knowledge Center article CTX310743.

Restart schedule maximum delay timer (PowerShell only). If a scheduled restart of machines in a Delivery Group doesn't begin because of a site database outage, you can specify how long to wait beyond the scheduled start time. If the database connection is restored during that interval, the restarts begin. If the connection isn't restored during that interval, the restarts don't begin. For details, see Scheduled restarts delayed due to database outage.

Vertical load balancing (PowerShell only). Previously, the service used horizontal load balancing for all RDS launches, which assigns incoming load to the least-loaded RDS machine. That remains the default. Now, you can use PowerShell to enable vertical load balancing as a site-wide setting.

When vertical load balancing is enabled, the broker assigns incoming load to the most-loaded machine that has not reached a high watermark. This saturates existing machines before moving on to new machines. As users disconnect and free up existing machines, new load is assigned to those machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, horizontal load balancing is enabled. To view, enable, or disable vertical load balancing, the `Get-BrokerSite`, and `Set-BrokerSite` cmdlets now support the `UseVerticalScalingForRdsLaunches` setting. For more information, see Load manage machines in Delivery Groups.

December 2019

New and enhanced features

Service for Citrix Service Providers (CSP). CSPs can now onboard tenant customers to the Virtual Apps and Desktops service, configure customer administrator access to the service, and provide shared or dedicated workspaces to customers' users using federated domains. For more information, see Citrix Virtual Apps and Desktops service for Citrix Service Providers.

Support for determining why a machine is in maintenance mode (PowerShell only). Using PowerShell, you can now determine why a machine is in maintenance mode. To do so, use the parameter `-MaintenanceModeReason`. The feature is useful for administrators to troubleshoot issues with machines in maintenance mode. For details, see `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/Broker/Get-BrokerMachine/>`.

Autoscale. Autoscale now provides the capability to create machines and delete them dynamically. You can use the capability by using a PowerShell script. The script helps you dynamically scale up or down the number of machines in the Delivery Group based on the current load conditions. For more information, see Dynamically provision machines with Autoscale.

November 2019

New and enhanced features

GroomStartHour. Monitor now supports **GroomStartHour** - a new configuration that helps administrators to determine the time of the day that grooming should start running. For more information, see the Citrix Virtual Apps and Desktops SDK documentation.

OData Pagination. Monitor now supports **OData pagination**. All OData v4 endpoints return a maximum of 100 records per page with a link to the next 100 records in the response. For more information, see Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

October 2019

New and enhanced features

App-V. App-V functionality is now available in Citrix Cloud. You can add App-V packages to the Delivery Controller in your Citrix Cloud configuration, in either single- or dual admin mode. The *Virtual Apps and Desktops Service App-V package discovery module*, available in Citrix Downloads, allows you to import App-V packages and register Microsoft App-V servers. The apps they contain are then available to your users. This PowerShell module allows you to register Microsoft App-V Management and Publishing Servers using DNS URLs, avoiding the need for servers behind load balancing mechanisms to be registered using their actual machine URL. For more information, see Citrix Virtual Apps and Desktops service discovery module for App-V packages and servers.

Google Cloud Platform. Citrix Virtual Apps and Desktops service now adds support for using Machine Creation Services (MCS) to provision machines on the Google Cloud Platform (GCP). For more information, see Google Cloud Platform virtualization environments.

September 2019

New and enhanced features

VDA support for Azure Virtual Desktop. For supported operating systems and VDA versions see VDAs in an Azure Virtual Desktop environment.

Enhanced power policy. In earlier releases, a VDI machine transitioning to a time period where an action (disconnect action="**Suspend**" or "**Shutdown**") was required remained powered on. This scenario occurred if the machine disconnected during a time period (peak or off-peak times) where no action (disconnect action="**Nothing**") was required.

Starting with this release, Autoscale suspends or powers off the machine when the specified disconnection time elapses, depending on the disconnect action configured for the destination time period. For more information, see Power manage VDI machines transitioning to a different time period with disconnected sessions.

Machine catalogs: Tags. You can now use PowerShell to apply tags to machine catalogs. For more information, see Apply tags to machine catalogs.

Session startup duration. Monitor now displays the session startup duration divided into Workspace App Session Startup and VDA Session Startup time periods. This data helps you to understand and troubleshoot high session startup duration. Further, the time duration for each

© 1997–2026 Citrix Systems, Inc. All rights reserved.

phase involved in the session startup helps in troubleshooting issues associated with individual phases. For example, if the Drive Mapping time is high, you can check if all the valid drives are mapped properly in the GPO or script. This feature is available on VDAs 1903 or later. For more information, see Diagnose session startup issues.

August 2019

New and enhanced features

Session Auto Reconnect. The Sessions page on the Trends tab now includes information about the number of auto reconnects. Auto reconnects are attempted when the Session Reliability or Auto Client Reconnect policies are in effect. The auto reconnect information helps you view and troubleshoot network connections having interruptions, and also analyze networks having a seamless experience.

The drilldown provides additional information like Session Reliability or Auto Client Reconnect, time stamps, Endpoint IP, and Endpoint Name of the machine where the Workspace app is installed. This feature is available for Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Receiver™ for Windows, and Citrix Receiver for Mac. This feature requires VDAs 1906 or later. For more information, see:

- Sessions
- Auto client reconnect policy settings
- Session reliability policy settings
- Session Auto Reconnect

July 2019

New and enhanced features

Configuration Logging. You can now use the Remote PowerShell SDK to periodically delete Configuration Logging database content. For details, see Schedule periodic data deletion.

Autoscale. Autoscale now provides the flexibility to power manage only a subset of machines in a Delivery Group. This feature can be useful in cloud bursting use cases, where you want to use on-premises resources to handle workloads before cloud-based resources address other demands (that is, burst workloads). For more information, see Restrict Autoscale to certain machines in a Delivery Group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Local App Access and URL redirection. Citrix Studio now lets you add the Add Local App Access Application option to the Studio user interface for your Site by using the PowerShell SDK. For more information, see Provide access only to published applications.

Operating system name changes. Operating system names on the **Create Machine Catalog > Machine Catalog Setup > Operating System** and the **Monitor** pages have changed:

- Multi-session OS (formerly Server OS): The multi-session OS machine catalog provides hosted shared desktops for a large-scale deployment of standardized Windows multi-session or Linux OS machines.
- Single-session OS (formerly Desktop OS): The single-session OS machine catalog provides VDI desktops ideal for various users.

Citrix Profile Management duration in Profile Load. Monitor now includes profile processing duration in the Profile Load bar of the Logon duration chart. This is the duration Citrix Profile Management takes to process user profiles. This information helps administrators to troubleshoot high profile load durations with greater accuracy. This enhancement is available on VDAs 1903 and later. For more information, see Profile Load.

Desktop probing. Desktop probing is a feature of the Citrix Virtual Apps and Desktops service. It automates health checks of virtual desktops published on a site, which improves user experience. To initiate desktop probing, install and configure the Citrix Probe Agent on one or more endpoints. Desktop probing is available for Premium licensed Sites. This feature requires Citrix Probe Agent 1903 or later. For more information, see Application and Desktop Probing.

NOTE:

Citrix Probe Agent now supports TLS 1.2.

June 2019

New and enhanced features

Restrict by tags. Tags are strings that identify items such as machines, applications, desktops, Application Groups, and policies. After creating a tag and adding it to an item, you can tailor certain operations to apply to only items that have a specified tag. For more information, see Application Groups and Tags.

Email Notifications. Citrix Virtual Apps and Desktops service sends email notifications related to alerting and probing directly. This eliminates the need to configure the SMTP email server. The

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Notification Preferences box is enabled by default and Citrix Cloud sends alert notifications to the email addresses provided in the **Notification Preferences** section. Ensure that the email address `donotreplynotifications@citrix.com` is white-listed in your email setup.

May 2019

New and enhanced features

Autoscale. Autoscale is a feature of Citrix Virtual Apps and Desktops service that provides a consistent, high-performance solution to proactively power manage your machines. It aims to balance costs and user experience. Autoscale incorporates the deprecated Smart Scale technology into the Studio power management solution. For more information, see Autoscale. You can monitor the metrics of Autoscale-managed machines from the Trends pages on the **Monitor** console. For more information, see Monitor Autoscale-managed machines.

February 2019

New and enhanced features

Hypervisor alerts monitoring. Alerts from Citrix Hypervisor and VMware vSphere are now displayed on the **Monitor** > **Alerts** tab to help monitor the following states/parameters of hypervisor health:

- CPU usage
- Memory usage
- Network usage
- Hypervisor connection unavailable
- Disk usage (vSphere only)
- Host connection or power state (vSphere only)

For more information, see the Hypervisor alerts monitoring section in Alerts and Notifications.

Communications over earlier TLS versions. To improve the security of the service, Citrix will block any communication over Transport Layer Security (TLS) 1.0 and 1.1 as of March 15, 2019, allowing only TLS 1.2 communications. For more information, see TLS versions. For comprehensive guidance, see CTX247067.

Application Groups. Application Groups let you manage collections of applications. You can create Application Groups for applications shared across different Delivery Groups or used by a subset of users within Delivery Groups. For more information, see Create Application Groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logon Performance - Profile Drilldown. The **Logon Duration** panel on the **User Details** page within **Monitor** now includes information on the **Profile load phase** drilldown of the logon process. Profile drilldown provides useful information about user profiles for the current session that can help administrators troubleshoot high profile load issues. A tool tip with the following user profiles information is displayed:

- Number of files
- Profile size
- Number of large files

A detailed drill-down provides information about the individual folders, their size, and the number of files. This feature is available on VDAs 1811 and later. For more information, see Diagnose user logon issues.

Microsoft RDS license health. Monitor the Microsoft RDS (Remote Desktop Services) license status on the **Machine Details** panel on the Machine Details and the User Details page for Server OS machines. An appropriate message is displayed for the license status. You can hover over the info icon to see further details. For more information, see the Microsoft RDS license health section in Troubleshooting Machines.

Application Probing. This feature automates the assessment of the health of Virtual Apps published in a Site.

To initiate application probing:

- On one or more endpoint machines, install the Citrix Application Probe Agent
- Configure the Citrix Application Probe Agent with the credentials of Citrix Workspace and Citrix Virtual Apps and Desktops service.
- Configure the applications to be probed, the endpoint machines to run the probe on, and the scheduled probe time in **Monitor** > **Configuration** of the Citrix Virtual Apps and Desktops service.

The agent tests the launch of selected applications via Citrix Workspace and reports back the probe results on the **Monitor** console of Citrix Virtual Apps and Desktops service in:

- the Applications page – the last 24-hours' data and the **Trends** > **Application Probe Results** page
- the historical probe data along with the stage when the probe failure occurred - Workspace Reachability, WorkspaceAuthentication, WorkspaceEnumeration, ICA download, or Application launch

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The failure report is emailed to configured email addresses. You can schedule application probes to run during off-peak hours across multiple geographical locations. In that way, you can use the results to proactively troubleshoot issues related to provisioned applications, hosting machines, or connections before the users experience them. For more information, see Application and Desktop Probing.

January 2019

New and enhanced features

Delegated Administration with custom scope. Monitoring now supports custom scope for built-in delegated administrator roles. For more information on the available built-in roles for monitoring and how to assign them, see Delegated administrator roles.

December 2018

New and enhanced features

The date after which Citrix will block communication over Transport Layer Security (TLS) 1.0 and 1.1 has changed from December 31, 2018 to January 31, 2019. For details, see Deprecation of TLS versions.

November 2018

New and enhanced features

Machine historical data available using OData API: Historical data containing machine analytics is now available through the OData API. This data is collected on an hourly basis and rolled up for the day.

- Number of powered on machines (for power managed machines)
- Number of registered machines
- Number of machines in maintenance mode
- Total number of machines

The data is aggregated for the time period during which the Monitoring Service is running. For more information on the usage of the OData API and examples, see Citrix Monitor Service 7 1808. The database schema is available at Monitor Service Schema.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logon Performance - Interactive session drilldown: The **Logon Duration** panel on the **User and Session Details** view includes information on the **Interactive Session** phase of the logon process. The time taken for each of the three subphases (**Pre-userinit**, **Userinit**, and **Shell**) is displayed on the **Interactive Session** bar as a tooltip. This provides more granular troubleshooting and remediation of this phase of the logon. The cumulative time delay between the subphases and a link to the documentation is also provided. This feature is available on Delivery Controller version 7 1808 and later. The **Interactive Session** drilldown bar shows the time duration for the current session only. For more information, see Diagnose user logon issues.

Logon Performance - GPO drilldown: The **Logon Duration** panel on the **User and Session** details view contains the GPO (Group Policy Objects) duration. This is the total time taken to apply the GPOs on the virtual machine during the logon process. Now, you can see the drilldown of each policy applied as per CSEs (Clients-Side Extension) as a tool tip on the GPO bar. For each policy application, the drilldown displays the status and the time taken. This additional information eases troubleshooting and remediation of issues involving high GPO duration. The time durations in the drilldown represent the CSE processing time only and do not add up to the total GPO time. This feature is available on Delivery Controller version 7 1808 and later. For more information, see Diagnose user logon issues.

Fixes

Custom report queries saved during monitoring are not available after a Cloud upgrade.

October 2018

New and enhanced features

Applications: Limit per machine. You can now limit the number of application instances per machine. This limit applies to all machines in the Site. This limit is an addition to the existing application limit for all users in the Delivery Group and the limit per user. This capability is available only through PowerShell, not in Studio. For details, see Configure application limits.

Windows Server 2019. You can now install VDAs for multi-session OS (formerly VDAs for Server OS) on Windows Server 2019 machines, as noted in System requirements.

September 2018

New and enhanced features

Delegated Administration. With Delegated Administration, you can configure the access permissions that all of your administrators need, in accordance with their role in your organization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For details, see Delegated Administration. Monitoring supports allocation of built-in roles. Built-in roles are available with full scope. For more information about built-in roles for monitoring and how to assign them, see Delegated administrator roles.

Configuration Logging. Configuration Logging allows administrators to keep track of configuration changes and administrative activities. For details, see Configuration Logging.

Several PowerShell cmdlets in the Remote PowerShell SDK that were previously disabled are now enabled, for use with Configuration Logging:

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

Local Host Cache. Local Host Cache is now fully available. Local Host Cache enables connection brokering operations to continue when a Cloud Connector in a resource location cannot communicate with Citrix Cloud. For details, see Local Host Cache.

Citrix Provisioning. To provision VDAs, you can now use Citrix Provisioning or the existing Machine Creation Services. For Citrix Provisioning information specific to the cloud environment, see Citrix Provisioning managed by Citrix Cloud.

Fixes

In earlier versions, when using Azure on-demand provisioning, all VMs were deleted when powered-off. Now, only pooled VMs are deleted. Persistent (dedicated) VMs are not deleted when powered-off.

August 2018

- **New product names**

  If you've been a Citrix customer or partner for a while, you'll notice new names in our products and in this product documentation. If you're new to this Citrix product, you might see different names for a product or component.

  The new product and component names stem from the expanding Citrix portfolio and cloud strategy. Articles in this product documentation use the following names.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Citrix Virtual Apps and Desktops:** Citrix Virtual Apps and Desktops offers a virtual app and desktop solution, provided as a cloud service and as an on-premises product, giving employees the freedom to work from anywhere on any device while cutting IT costs. Deliver Windows, Linux, web, and SaaS applications or full virtual desktops from any cloud: public, on-premises, or hybrid. Virtual Apps and Desktops was formerly XenApp and XenDesktop.
- **Citrix Workspace app:** The Citrix Workspace app incorporates existing Citrix Receiver technology and other Citrix Workspace client technologies. It has been enhanced to deliver more capabilities to provide end users with a unified, contextual experience where they can interact with all the work apps, files, and devices they must do their best work. For more information, see this blog post.
- **Citrix SD-WAN™:** NetScaler SD-WAN, a crucial technology for our customers and partners transforming their branch networks and WANs with cloud technology, is now Citrix SD-WAN.
- **Citrix Secure Web Gateway™:** As the Citrix Networking portfolio expands, we're proud to offer our robust Citrix Secure Web Gateway Service, previously known as NetScaler Secure Web Gateway.
- **Citrix Gateway:** Our robust NetScaler® Unified Gateway, which allows secure, contextual access to the apps and data you must do your best work, is now Citrix Gateway.
- **Citrix Content Collaboration™ and Citrix Files for Windows:** The advanced access, collaboration, workflows, rights management, and integration features of ShareFile are now available in the Citrix Content Collaboration component set in our secure, contextual, integrated Citrix Workspace. Citrix Files for Windows allows you to access your Content Collaboration files directly through a mapped drive, providing a native Windows Explorer experience.
- **Citrix Hypervisor**: The technology from XenServer for virtualization infrastructure, based on the XenProject hypervisor, is now Citrix Hypervisor.

Here's a quick recap:

IS	WAS
Citrix Virtual Apps and Desktops	XenApp® and XenDesktop
Citrix Workspace app	Incorporates Citrix Receiver and extensive enhancements
Citrix SD-WAN	NetScaler SD-WAN

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IS	WAS
Citrix Secure Web™ Gateway	NetScaler Secure Web Gateway
Citrix Gateway	NetScaler Unified Gateway
Citrix Content Collaboration	ShareFile
Citrix Files for Windows	ShareFile Desktop App, ShareFile Sync, ShareFile Drive Mapper
Citrix Hypervisor	XenServer
Citrix Provisioning	Citrix Provisioning Services

Implementing this transition in our products and their documentation is an ongoing process.

- In-product content might still contain former names. For example, you might see instances of earlier names in console text, messages, and directory/file names.
- It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.
- Related product documentation and other resources (such as videos and blog posts) that are linked from this product's documentation might still contain former names.
- For Citrix Hypervisor: The new name is used on the Citrix website and in informational product materials from September 2018. You will also see the new name on the administrator consoles of some Citrix products, such as Citrix Virtual Apps and Desktops. The XenServer product release and technical documentation materials continue to use XenServer 7.x until early 2019.

Your patience during this transition is appreciated.

For more detail about our new names, see `<https://www.citrix.com/about/citrix-product-guide/>`.

- **Product and component version number changes**

  Citrix installs and manages most of the Citrix Virtual Apps and Desktops components, so you won't be concerned with those version numbers. However, you might see version numbers when installing Cloud Connectors, and when installing or upgrading VDAs in resource locations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Apps and Desktops product and component version numbers are displayed in the format: **YYMM.*c.m.b***

- YYMM = Year and month when the product or component released. For example, a September 2018 release appears as 1809.
- c = Citrix Cloud release number for the month.
- m = Maintenance version (if applicable).
- b = Build number. This field is shown only on the About page of the component, and in the OS's feature for removing or changing programs.

For example, **Citrix Virtual Apps and Desktops 1809.1.0** indicates that the component released in September 2018. It is associated with Citrix Cloud release 1 in that month, and is not a maintenance version. Some displays show only the version's year and month: for example, **Citrix Virtual Apps and Desktops 1809**.

In earlier releases (7.18 and earlier), version numbers were displayed in the format: 7.*version*, where version incremented by one for each release. For example, the VDA release following XenApp and XenDesktop 7.17 was 7.18. Earlier releases (7.18 and earlier) will not be updated with the new numbering format.

- **Deprecation of TLS versions.** To improve the security of the Citrix Virtual Apps and Desktops service, Citrix will block any communication over Transport Layer Security (TLS) 1.0 and 1.1, effective December 31, 2018. For details, see Deprecation of TLS versions.
- **Google Cloud Platform virtualization environment.** The Citrix Virtual Apps and Desktops service supports the ability to manually power cycle Virtual Apps and Desktops VMs on the Google Cloud Platform (GCP). For more information, see Google Cloud Platform virtualization environments.

July 2018

- **Export of Filters data.** You can now export real-time monitoring data on the **Monitor** > **Filters** tab to CSV format files. The export feature is available from the Machines, Sessions, Connections, and Application Instances Filters pages. You can select a predefined custom filter or select suitable filter criteria, choose required columns on the table, and export the data. Data of up to 100,000 records can be exported. The exported CSV files give a comprehensive view of the real-time data, and helps ease analysis of large data sets.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 2018

- **Azure Resource Manager connections.** In the Studio connection creation wizard, the Azure environment selection on the **Connection** page includes all Azure Clouds that are valid for your Azure subscription. General availability for Azure US Government Cloud and Azure Germany Cloud replaces the preview versions of those two environments in earlier releases.

May 2018

- **Azure Quick Deploy.** When your resource location uses Azure Resource Manager machines to deliver applications and desktops, you can now choose a deployment method:
  - Full Configuration: This existing method uses the Studio management console, which guides you through creating a machine catalog and then creating a Delivery Group.
  - Azure Quick Deploy: This new option offers a simpler interface that offers faster deployment of apps and desktops.
- **Citrix Health Assistant link.** The Machine Details page of an unregistered machine on the Monitoring console now contains a **Health Assistant** button. Currently, the button links to Troubleshoot machines and to the Knowledge Center article, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch where you can download the tool. Citrix Health Assistant is a tool to troubleshoot configuration issues in unregistered VDAs. The tool automates several health checks to identify possible root causes for common VDA registration, session launch, and time zone redirection configuration issues.
- **Interactive Session drilldown.** In the monitoring console, the **User Details view > Logon Duration** panel now includes information on the **Interactive Session** stage of the logon process. To provide more granular troubleshooting and remediation of this phase of the logon, **Interactive Session** now has three subphases: **Pre-userinit**, **Userinit**, and **Shell**. In this release, hovering over **Interactive Session** displays a tooltip showing the subphases and a link to the documentation. For a description of the subphases and how to improve the performance of each phase, see Diagnose user logon issues.

March 2018

- **Application instance prediction (Preview feature).** This is the first monitoring feature based on predictive analytics. Predicting resource usage patterns is important for administrators to organize resources and the required number of licenses on each resource. The Application instance prediction feature indicates the number of hosted application instances that are likely to be launched per Site or Delivery Group over time. Machine learning algorithms based on

© 1997–2026 Citrix Systems, Inc. All rights reserved.

data models created with existing historical data are used to do the prediction. Tolerance level indicates the prediction quality.

For more information see Application instance prediction in Monitor. Submit your feedback regarding the usefulness and usability of this feature in the Citrix Cloud discussion forum.

- **Delivery Groups APIs - Preview**

  The Delivery Groups APIs Preview provides a set of REST APIs that you can use to automate the management of Delivery Groups. The complete set of available APIs can be viewed and tried out in the Citrix Cloud API documentation at `<https://developer.cloud.com/>`.

- **Web Studio authentication**

  The service management console on Citrix Cloud now uses a bearer token to authenticate customers. The bearer token is required to authenticate access to the Delivery Groups REST API.

- **Access Monitor Service data using OData Version 4 API (Preview feature)**

  You can create your customized monitoring and reporting dashboards based on the Monitor Service data by using the OData V.4 endpoint. OData V.4 is based on ASP .Net Web API and supports aggregation queries. Use your Citrix Cloud user name and bearer token to access the data with the V4 endpoint. For more information and examples, see Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

  Share your feedback on the utility of this feature in the Citrix Cloud discussion forum.

Fixes

- You can rename, move, and delete application folders.

January 2018

- **RDS license check.** Creation of machine catalogs containing Windows Server OS machines now includes an automatic RDS license check. Any RDS license issues found are displayed, so that you can take the appropriate steps to prevent a gap in service. For details, see Create machine catalogs.
- **Access to machine console from Monitor.** The Machine Details panel from Monitor now provides access to consoles of machines hosted on the XenServer hypervisor version 7.3. You can now troubleshoot issues in VDAs directly from Monitor. For more information, see Machine Console access in Troubleshoot machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

December 2017

New and enhanced features

- **Citrix Workspace.** Citrix Workspace is now available for **new** XenApp and XenDesktop Service customers. For more information, see Workspace Configuration.
- **Applications Analytics.** You can now analyze and monitor the performance of applications efficiently with the new Application Analytics page available from **Monitor** > **Applications** tab. The page provides a consolidated view of the health and usage of all applications published on your Site. It shows metrics such as the number of instances per application, and faults and errors associated with the published applications. This feature requires VDAs Version 7.15 or later.

  For more information, see Application Analytics section in Monitor.

November 2017

New and enhanced features

- **Local Host Cache.** Local Host Cache enables connection brokering operations to continue when a Cloud Connector in a resource location cannot communicate with Citrix Cloud. For details, see Local Host Cache.
- **Azure Managed Disks.** Azure Managed Disks are now used by default for MCS-provisioned VMs in Azure Resource Manager environments. Optionally, you can use conventional storage accounts. For details, see Microsoft Azure Resource Manager virtualization environments.
- **Help desk administrator.** When managing service administrators for a Citrix Cloud customer account, you now have a new choice: Help Desk Administrator. A help desk administrator can access the Monitor functions on the service. For details, see Manage.

Fixes

- You can now use the service management console wizard to create a Remote PC Access machine catalog. In earlier releases, you had to use a PowerShell cmdlet to create a catalog (as documented in CTX220737). Then, you had to return to the management console to create a Delivery Group. Now, you create the catalog and the Delivery Group sequentially on the management console.
- MCS-created catalogs can use existing Active Directory machine accounts.
- When monitoring a deployment, scrolling in a sorted **Trends > Sessions** table displays accurate results.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More information

- Known issues.
- For information about third-party software that is included in the service, see Third party notifications.

Known issues

Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) has the following known issues:

- Updating a vTPM-enabled master image for an MCS non-persistent machine catalog through a Nutanix AHV Prism Central connection triggers a VM recreation that might invalidate DNS reservations, and necessitate re-enrollment for software utilizing MAC addresses for licensing.
- When using a machine profile that has multiple network interfaces (NICs) with Accelerated Networking enabled, ensure that the selected VM size supports Accelerated Networking on all NICs. Some Azure VM sizes (for example, Standard_D2ads_v5) restrict Accelerated Networking to a single NIC. If the machine profile enables Accelerated Networking on more NICs than the VM size allows, machines fail to power on with the error `VmSizeRestrictedToSingleNicWithAcceleratedNetworkingEnable`. To resolve this, either select a VM size that supports Accelerated Networking on multiple NICs, or update the machine profile to enable Accelerated Networking on only one NIC.
- Adding a large batch of VMs to an MCS catalog using a Nutanix AHV Prism Central host connection might fail with an `OutOfMemory` error. To avoid this, reduce the number of VMs created in a single batch. We recommend adding a maximum of 10 VMs at a time.
- Hourly costs for certain Azure Windows Instance SKUs (for example, `Standard_DS*{_}v2{_}*`) are displayed as **Unavailable** in Studio. This occurs because our cost feature depends on the public Azure Resource Pricing API, and this API, by design, no longer provides pricing information for certain meter data it has deprecated from its own reporting. This limitation affects the display of retail and effective prices for the Windows Instance SKUs within the system.
- If the user's Azure UPN contains a dot as the twentieth character, the Windows Server VDA is unable to create a local user account.
- When creating an MCS machine catalog in a Red Hat OpenShift virtualization environment, you can’t use a master image and a machine profile that have different operating system types. This is due to how Red Hat OpenShift manages each OS type. Therefore, using a Windows VM as the master image with a non-Windows (example, Linux) VM as the machine profile, or the other way around, is not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Currently, the VMs created using `InstanceType` are not supported as a master image.
- When the metainstaller is used to install the Citrix Virtual Apps and Desktops components on a machine running Windows Server 2025, then MsiInstall events are not being written to the event logs.
- After you create a backup and navigate to the **Components** tab for that selected backup, you see empty data for a component that has a resource after you click **View component members**.
- When trying to restore AWS, Azure, GCP, and XenServer® hosting connections, the **Restore count** on the **Restore Progress** page is **1** and displays only the restore action result of XenServer.
- After you create a backup, the **Hosting Connections** component count on the **Backup progress** page is displayed as **0**.
- In a VMware environment hosted on AWS, the MCS machine catalog creation fails if the master image is vTPM enabled. This issue affects all Citrix Virtual Apps and Desktops versions and is due to a problem in the VMware environment. For assistance, contact VMware support.
- If you use Microsoft Entra Domain Services: End user logon UPNs must contain the domain name that was specified when enabling Microsoft Entra ID Domain Services. Logons cannot use UPNs for a custom domain you create, even if that custom domain is designated as primary.

For issues related to current VDAs, see Known issues.

Deprecations and removals

This article gives you advanced notice of Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) features that are being phased out, so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when features are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality. For details about product lifecycle support, see the Product Lifecycle Support Policy article.

NOTE:

Citrix Virtual Apps and Desktops deprecations and removals are described in their own Deprecation article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deprecations and removals

The following list shows the Citrix DaaS™ features that are deprecated or removed.

- *Deprecated* items are not removed immediately. Citrix® continues to support them but they will be removed in a future release.
- *Removed* items are removed, or no longer supported, in Citrix DaaS. Dates in **bold** face indicate the latest updates.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	REMOVED IN RELEASE	ALTERNATIVE
Support for the third-party HPE Moonshot Machine Manager plug-in	May 2024	-	Use Citrix-managed HPE Moonshot plug-in
The **Last Boot Time (UTC)** column in Studio and the **LastBootTime** field in **Get-ProvVM** and **Get-ProvVMDetails** responses	July 2026	-	-
Studio UI option for App-V full infrastructure	April 2026		Migrate to the App-V Single Admin model
Per-delivery-group license overrides (multi-type licensing)	April 2026	Citrix DaaS uses site-level license settings only. Delivery group overrides are ignored and the **License Assignment**	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	REMOVED IN RELEASE	ALTERNATIVE
		step in the Create and Edit Delivery Group wizards is removed. For more information, see Licenses.	
Support for `Get-BrokerMachine`	July 2025	Use `Get-BrokerMachineV2`	
Support for `$XDSDKAuth` for SDK Authentication	June 2025	June 2025	Run `Get-XDAuthentication -ProfileName WindowsCurrentUser`
Support for the following `-AcctADAccount` PowerShell commands • New-AcctADAccount • Add-AcctADAccount • Update-AcctADAccount	December 2024		Use the -AcctIdentity PowerShell commands • New-AcctIdentity • Add-AcctIdentity • Update-AcctIdentity • Remove-AcctIdentity • Unlock-AcctIdentity

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	REMOVED IN RELEASE	ALTERNATIVE
• Remove-AcctADAccount • Unlock-AcctADAccount • Get-AcctADAccount			• Get-AcctIdentity
Support for `Repair-AcctADAccount` PowerShell command	December 2024		Use the following commands • `Repair-AcctIdentity`: To repair identity accounts without changing the current state of them. This can repair existing in-used identity accounts for existing provisioned VMs. For

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	REMOVED IN RELEASE	ALTERNATIVE
			example, `repair userCertificate` attributes for Microsoft Entra hybrid joined identity accounts. The `Repair identity info` (including machine password/ trust key pair) for AD joined identity accounts. • `Reset-AcctIdentity`: To reset identity accounts to initial states (For example,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	REMOVED IN RELEASE	ALTERNATIVE
			from tainted to available). This can put any tainted identity accounts back to pool as available identity accounts.
Support for `-ResetIdentityInfo` PowerShell command	October 2024		Use `-Recreate` to recreate the identity disk. For information, see Repair the identity information of active computer accounts.
Support for configuring the MCS I/O write-back cache to include only a disk cache and no memory cache	February 2024	January 2025	NA
Support for Azure catalogs created before	February 2024		Recreate Azure legacy catalog VMs. The

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	REMOVED IN RELEASE	ALTERNATIVE
on-demand provisioning feature ("legacy" catalogs)			catalogs are provisioned as on-demand and help to save storage cost.
Support for Citrix Connector 3.1 for System Center Configuration Manager	December 2023	August 2025	Do image or application update manually.
Support for using a master image in a region different from the region where the catalog is created	December 2023		Use Azure Compute Gallery to replicate the master image to the required region.
Support for AWS volume worker	November 2023	June 2025	Use Direct disk upload and download. See Direct disk upload and download.
Support for `Leave user management to Citrix Cloud` used in creating delivery groups	September 2023	September 2023	
Support for `AwsCaptureInstancePropert`	August 2023		Use a machine profile. See Create a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	REMOVED IN RELEASE	ALTERNATIVE
`ies` used in AWS environments			catalog using a machine profile.
Support for VMware vSphere 6.7		June 2023	Use higher versions for VMware vSphere.
`Schedule-ProvVMUpdate` PowerShell command	April 2023		Use `Set-ProvVMUpdateTimeWindow` command.
`Request-ProvVMUpdate` PowerShell command	April 2023		Use `Set-ProvVMUpdateTimeWindow` command with `-StartsNow` and `-DurationInMinutes -1` parameters.
`Cancel-ProvVMUpdate` PowerShell command	April 2023		Use `Clear-ProvVMUpdateTimeWindow` command.
`DedicatedTenancy` parameter used in `New-ProvScheme` command	March 2023		Use `TenancyType` parameter.
Unmanaged disk to create	June 2022		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	REMOVED IN RELEASE	ALTERNATIVE
VM in the Azure environment			
Support for four AWS specific commands: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress`, and `Grant-HypSecurityGroupIngress`	May 2022		
`StorageAccountType` parameter used in Azure environments	April 2022		Use `StorageType`.
Legacy console (MMC-based console)	July 2021	November 2021	Use **DaaS > Manage** to access the full range of configuration and management actions.
Azure Quick Deploy	September 2020		Use Quick Deploy.
Ability to import Citrix	August 2020	February 2021	Use the Citrix Provisioning

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	REMOVED IN RELEASE	ALTERNATIVE
Provisioning target devices to create catalogs in Citrix Studio.			Export Devices Wizard to push Citrix Provisioning VMs into Delivery Controllers/ MCS for catalog creation. See Export Devices Wizard.

Features in preview

Features in preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in preview but welcomes feedback for improving them. Citrix might act on feedback based on its severity, criticality, and importance.

List of features in preview

The following table lists the features in the preview.

TITLE	ENABLEMENT FORM (CLICK THE ICON)	FEEDBACK FORM (CLICK THE ICON)
Citrix Integration with Azure Local for Linux workload		NA
Secure Private Access integration with Monitor	NA	NA
Enrollment of Hybrid Entra ID joined non-persistent VMs into Microsoft Intune		NA
VUS Multi Release Support	NA	NA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Integration with Azure Local for Linux workload

Azure Local is a hyper-converged infrastructure (HCI) solution that connects the on-premises system to Azure for cloud-based services, monitoring, and management.

With this feature, MCS supports Azure Local as a new platform, and thus supports:

- Provisioning of Azure Arc-enabled Linux VMs on Azure Local.
- Power management of Linux VMs created on Azure Local.

For more information, see Citrix Integration with Azure Local for Linux workload.

Secure Private Access integration with Monitor

This preview allows admin to monitor and troubleshoot all Secure Private Access sessions in Monitor.

Available actions include viewing the details of the following:

- Secure Private Access active sessions for a user under the Select a Session popup > Active Sessions tab
- Secure Private Access failed or blocked enumerations and failed app launches under the Select a Session popup > Denied Access tab
- Session and application details view for active and failed app launches, as well as for failed and blocked enumerations

For more information, see Secure Private Access integration with Monitor (Preview) page.

Enrollment of Hybrid Entra ID joined non-persistent VMs into Microsoft Intune

With this preview, you can now enroll Hybrid Entra ID joined non-persistent VMs into Microsoft Intune (with Configuration Manager) for co-management. This feature applies to single and multi-session non-persistent VMs and on all hypervisors and cloud services, ensuring uniform device management across your infrastructure. To avail the feature, the VDA version must be 2407 or later. For more information, see Enrollment of Hybrid Entra ID joined non-persistent VMs into Microsoft Intune.

VUS Multi Release Support

Previously VUS only allowed upgrades to the most recent version of the VDA released in each of the Upgrade Track. This new tech preview feature enables you to upgrade to new as well as previously released versions of the VDA. This feature is supported for catalog level Upgrades and individual machine Level VDA upgrades. For more information, see VUS Multi Release Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Preview to general availability (GA)

- Tenant co-management for CSP multitenant DaaS
- Integration with Nutanix Prism Central on AHV
- Image management
- Support for creating and managing Azure confidential VMs using Full Configuration
- Support for Citrix-managed HPE Moonshot plug-in
- Azure hibernation
- Policy sets
- Cost savings
- Diagnose historical user sessions
- Infrastructure monitoring
- Infrastructure policy
- Monitor multiple Citrix DaaS instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System requirements

Introduction

System requirements for components that are not covered here (such as Citrix Workspace™ app and Citrix Provisioning™) are described in their respective documentation.

Specific recommendations for sizing VMs that deliver desktops and applications cannot be provided because of the complex and dynamic nature of hardware offerings. Every deployment has unique needs. Generally, sizing a VM is based on the hardware and not the user workloads (except for RAM; you need more RAM for applications that consume more.) The Citrix Tech Zone contains the latest guidance on VDA sizing.

IMPORTANT:

VDA versions mentioned in this article are subject to the Citrix product lifecycle. For more information, see the Product Matrix on the Citrix web site.

For more information about using LTSR VDAs with Citrix DaaS, see CTX205549.
Remember: In a Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) deployment, you don't need to install or manage the core components (Delivery Controllers, the site database, or management and monitoring consoles). For Virtual Delivery Agent (VDA) installation guidance, see:

- Install VDAs
- Install VDAs using the command line.

Cloud Connectors

For details, see Cloud Connector Technical Details.

Hypervisor connectivity validation

To support the transition of hypervisor management (XenServer, VMware, AWS) from Cloud Connectors to the Cloud Delivery Controller, Citrix DaaS provides an automated connectivity

© 1997–2026 Citrix Systems, Inc. All rights reserved.

validation engine. This tool verifies that the service can reach your resource location endpoints without impacting production environments.

Pre-Migration validation

Before the plugin moves to the cloud, the system runs a health check in **Validation Mode** to identify configuration gaps in:

- **Networking:** Firewall rules, DNS resolution, and routing.
- **Security:** SSL/TLS certificate trust and handshakes.
- **Authentication:** Credential validity from the new execution context.

Actionable reporting

Validation results are surfaced directly in the **Studio UI** and **Migration Readiness Checks**. If a check fails, the system provides specific error details (e.g., connection timeouts or certificate mismatches) via:

- **Health Status Indicators:** Real-time visibility in the management console. See https://docs.citrix.com/en-us/citrix-daas/manage-deployment/vda-health-checks#run-health-checks-for-vdas
- **Event Logs:** Detailed records for pre-migration remediation.
- **Post-Migration Alerts:** Continuous monitoring of NGS-related setup issues.

VDAs in an Azure environment

Supported operating systems:

- Windows 11 multi-session
- Windows 11 single-session
- Windows 10 multi-session
- Windows 10 single-session
- Windows Server 2025
- Windows Server 2022 (requires minimum VDA 2106)
- Windows Server 2019
- Windows Server 2016

© 1997–2026 Citrix Systems, Inc. All rights reserved.

All VDAs that haven't reached end of life are supported for use with Citrix DaaS. For LTSR VDAs, we recommend using them with the latest Cumulative Update. For more information about the lifecycle of VDAs, see Citrix Product Matrix.

Windows Server 2012 R2 is supported only with VDA 1912 (and later CUs).

Windows Server requires Microsoft RDS licensing.

For information about Azure Virtual Desktop, see the Microsoft documentation.

VDAs in Amazon WorkSpaces Core Managed Instances

Supported operating systems:

- Windows 11 single-session
- Windows 10 single-session
- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Ubuntu Server 24.04 LTS
- Debian 12

VDA for single-session OS

The following information applies to the latest VDA release.

Supported operating systems:

- Windows 11
- Windows 10
    - For edition support, see CTX224843. That article also contains links to Citrix known issues with the supported Windows versions.
    - Desktop composition redirection and legacy graphics mode are not supported on Windows 10.

Requirements:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microsoft .NET Framework 4.8 is installed automatically, if it (or a later version) is not already installed.
- Microsoft Visual C++ 2015-2019 Redistributable.
  - If the machine contains an earlier version of that runtime (such as 2015-2017), the Citrix® installer upgrades it.
  - If the machine contains a version earlier than 2015, Citrix installs the newer version in parallel.

Remote PC Access uses this VDA, which you install on physical office PCs. This VDA supports Secure Boot for Citrix Virtual Desktops™ Remote PC Access.

Several multimedia acceleration features (such as HDX™ MediaStream Windows Media Redirection) require that Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features are not installed and do not work. Do not remove Media Foundation from the machine after installing the Citrix software. Otherwise, users cannot log on to the machine. On most supported Windows desktop OS editions, Media Foundation support is already installed and cannot be removed. However, N editions do not include certain media-related technologies. You can obtain that software from Microsoft or a third party.

More information:

- For Linux VDA information, see the Linux Virtual Delivery Agent product documentation.
- To use the server VDI feature, you can use the command line interface to install a single-session VDA on a supported Windows Server machine. See Server VDI for guidance.
- For information about installing a VDA on an older machine, see Earlier operating systems.
- See also VDAs in an Azure Virtual Desktop environment.

VDA for multi-session OS

The following information applies to the latest VDA release.

Supported operating systems:

- Windows Server 2025 (requires minimum VDA 2407)
- Windows Server 2022 (requires minimum VDA 2106)
- Windows Server 2019, Standard and Datacenter Editions
- Windows Server 2016, Standard and Datacenter Editions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows 11
- Windows 10 (64-bit) all supported versions

The installer automatically deploys the following requirements:

- Microsoft .NET Framework 4.8 is installed automatically, if it (or a later version) is not already installed.
- Microsoft Visual C++ 2015-2019 Redistributable.
  - If the machine contains an earlier version of that runtime (such as 2015-2017), the Citrix installer upgrades it.
  - If the machine contains a version earlier than 2015, Citrix installs the newer version in parallel.

The installer automatically installs and enables Remote Desktop Services role services, if they are not already installed and enabled. This triggers a restart.

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that the Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features are not installed and do not work. Do not remove Media Foundation from the machine after installing the Citrix software. Otherwise, users cannot log on to the machine. On most Windows Server versions, the Media Foundation feature is installed through the Server Manager. However, N editions do not include certain media-related technologies. You can obtain that software from Microsoft or a third party.

If Media Foundation is not present on the VDA, these multimedia features do not work:

- Flash Redirection
- Windows Media Redirection
- HTML5 Video Redirection
- HDX RealTime Webcam Redirection

More information:

- For Linux VDA information, see the Linux Virtual Delivery Agent articles.
- For information about installing a VDA on a Windows operating system that is no longer supported, see Earlier operating systems.
- See also VDAs in an Azure Virtual Desktop environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hosts / virtualization resources

The following host/virtualization resources (listed alphabetically) are supported. Where applicable, the *major.minor* versions are supported, including updates to those versions. CTX131239 contains the most current hypervisor version information, plus links to known issues.

- **Amazon Web Services (AWS)**
  - You can provision applications and desktops on supported Windows server operating systems.
  - The Amazon Relational Database Service (RDS) is not supported.

  For more information, see AWS cloud environments.
- **Amazon WorkSpaces Core Managed Instances**

  For more information, see AWS cloud environments.
- **XenServer (formerly Citrix Hypervisor™)**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see XenServer virtualization environments.
- **Google Cloud Platform**

  For more information, see Google Cloud environments and Getting Started with Citrix DaaS on Google Cloud.
- **HPE Moonshot**

  For more information, see HPE Moonshot virtualization environments.
- **Microsoft Azure Resource Manager**

  For more information, see Microsoft Azure Resource Manager cloud environments.
- **Microsoft System Center Virtual Machine Manager**

  Includes any version of Hyper-V that can register with the supported System Center Virtual Machine Manager versions.

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Microsoft System Center Virtual Machine Manager virtualization environments.
- **Nutanix Prism Central on AHV**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Nutanix Prism Central on AHV.

- **Nutanix Acropolis with Prism Element**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Nutanix Prism Element on AHV.

- **NC2 for Citrix-managed Nutanix AHV Prism Central plug-in**

  For more information, see Nutanix AHV Prism Central.

- **NC2 for Nutanix Prism Element**

  For more information, see NC2 for Nutanix Prism Element.

- **Red Hat OpenShift**

  For more information, see Red Hat OpenShift virtualization environments.

- **VMware Cloud on AWS**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see VMware cloud on Amazon Web Services (AWS).

- **Azure VMware Solution (AVS)**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Azure VMware Solution (AVS) integration.

- **Google Cloud VMware Engine**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Google Cloud VMware Engine.

- **VMware vSphere(vCenter + ESXi)**

  No support is provided for vSphere vCenter Linked Mode operation.

  CTX131239 contains current version information, plus links to known issues.

  For more information, see VMware virtualization environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You must not install the VDA software on any Citrix DDC or StoreFront server. The VDA must be a stand-alone system. Installing multiple components on a single VM is only permissible when developing a proof-of-concept or when publishing the Studio admin console to administrators only. In this case you must ensure non-admin users do not have access to DDC/StoreFront VMs.

Active Directory functional levels

The following functional levels for the Active Directory forest and domain are supported:

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2

For more information about Active Directory, see Active Directory joined.

HDX technologies

For specific HDX feature support and requirements, see HDX.

Universal Print Server

The Universal Print Server comprises client and server components. The UpsClient component is included in the VDA installation. You install the UpsServer component on each print server where shared printers reside that you want to provision with the Citrix Universal™ Print Driver in user sessions.

The UpsServer component is supported on:

- Windows Server 2025
- Windows Server 2019
- Windows Server 2016

Requirements:

- Microsoft .NET Framework 4.8 (minimum)
- Microsoft Visual C++ 2015-2022 Redistributable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If the machine contains an earlier version of that runtime (such as 2015-2017), the Citrix installer upgrades it.
- If the machine contains a version earlier than 2015, Citrix installs the newer version in parallel.

For multi-session VDAs, user authentication during printing operations requires the Universal Print Server to be joined to the same domain as the VDA.

Standalone client and server component packages are also available for download.

For more information, see Provision printers.

Service connectivity

See System and Connectivity Requirements for Internet connection information. That information includes requirements that are common to most Citrix Cloud services, plus requirements specific to Citrix DaaS.

Other

- The Microsoft Group Policy Management Console (GPMC) is required if you store Citrix policy information in Active Directory rather than the site configuration database. The machine on which you install `CitrixGroupPolicyManagement_x64.msi` must have Visual Studio 2015 runtime installed. For more information, see the Microsoft documentation.
- This product supports PowerShell versions 3 through 5.
- For product components and features that you can install on Windows Servers, Server Core and Nano Server installations are not supported, unless noted.
- For details about resource limits in a deployment, see Limits.
- For supported StoreFront versions, see the StoreFront system requirements.
- For information about ports that Citrix DaaS uses, see Communications Ports Used by Citrix Technologies.
- For information about requirements when using the Quick Deploy management interface, see Requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limits

The values in this article indicate the limits of a single Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) instance. Citrix has extensively tested these limits and recommends for the best end user and admin experience. These limits are soft limits and not technically enforced (except for the number of Active Directory domains and the total number of VDAs per resource location). When the number of concurrent users exceeds 125,000, Citrix can scale and combine multiple Citrix DaaS instances, to deliver a unified experience at any scale.

The information in this article is dynamic. Check back frequently for updates. If you have current requirements that the published limits do not address, contact your Citrix® representative for assistance as early as possible.

Configuration limits

If policies exceed the limit, Citrix recommends using the Workspace Environment Management service or Active Directory Group Policy Objects (GPOs).

RESOURCE	LIMIT
Active Directory domains	250
Application folders	1,000
Application Groups	750
Applications	5,000
Catalogs	2,000
Delivery Groups	2,000
Host connections	200
Resource locations	250
Policies (Studio)	200

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE	LIMIT
Tags	20,000
VDAs	130,000

Resource location limits

The following table lists the limits for each resource location.

If your requirements exceed these limits, Citrix recommends using additional resource locations.

RESOURCE	LIMIT
Total VDAs (hard limit)	10,000
Total sessions	25,000
Active Directory domains	1
Host connections	40

Citrix Cloud Connectors are assigned to resource locations and link workloads to Citrix DaaS. For information about Cloud Connector limits, see Size and scale considerations for Cloud Connectors.

Provisioning limits

The provisioning limits in the following table are the Citrix recommended maximums for a single public provider subscription.

You are likely to reach quota limits from your public cloud vendor at lower levels. In such cases, contact the vendor to raise your subscription quota. For larger-scale deployments, Citrix recommends a hub-and-spoke model, where VDAs are distributed across multiple subscriptions and host connections.

For more information, see the following reference architectures:

- Citrix DaaS on AWS
- Citrix virtualization on Google Cloud
- Citrix DaaS on Azure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE	LIMIT
VDAs per AWS region	3,000
VDAs per Google Cloud Platform project	3,000
VDA per Microsoft Azure subscription per region	5,000

NOTE:

The limits are Citrix recommended.

Usage limits

For information about administrator roles and the differences between them, see:

- Manage Studio administrators
- Monitor (Director) administrators

RESOURCE	LIMIT
Concurrent Monitor (Director) full administrators	40
Concurrent Monitor (Director) help desk administrators	200
Concurrent Monitor (Director) session administrators	50
Concurrent Manage (Studio) cloud administrators	100
Concurrent Manage (Studio) help desk administrators	60
Concurrent end users	125,000
Resources published to a single user	250

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE	LIMIT
Session launches per minute	3,000

- Monitor (Director) supports the aggregation of up to four Citrix DaaS™ tenants (spokes) under a single tenant (hub).
- A help desk administrator on the hub instance can monitor and troubleshoot users, machines, endpoints, and transactions from all aggregated instances (hub and spokes) as per the Delegated Administration configuration on the specific instance.
- The number of concurrent administrators per Citrix DaaS instance is as per the Usage Limits table.

Limits change log

The following table tracks the configuration limit modification:

DATE	RESOURCE	DESCRIPTION
18 Feb 2025	Configuration limit of Resource locations	The limit increased from 200 to 250.
18 Feb 2025	Configuration limit of Active Directory domains	The limit increased from 100 to 250.
18 Aug 2025	Configuration limit of Tags	The limit increased from 10,000 to 20,000.
24 Feb 2025	Number of Application Groups	The limit increased from 250 to 750.
24 Feb 2025	Number of VDAs	The limit increased from 100,000 to 130,000.
12 Dec 2024	Resource locations	The limit increased from 100 to 200.
23 May 2024	VDAs per AWS account per region	The limit increased from 1500 to 3000.
22 Nov 2023	Active Directory domains	Limit increased from 85 to 100.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	RESOURCE	DESCRIPTION
	Catalogs	The limit increased from 1000 to 2000.
	Delivery Groups	The limit increased from 1000 to 2000.
	Resource locations	The limit increased from 85 to 100.
	Resource location -> Total sessions	Limit increased from 20,000 to 25,000.
04 Oct 2023	Tags	The limit increased from 500 to 10,000.
07 Dec 2023	Provisioning limits -> VDA per Microsoft Azure subscription per region	The limit increased from 2,500 to 5,000.

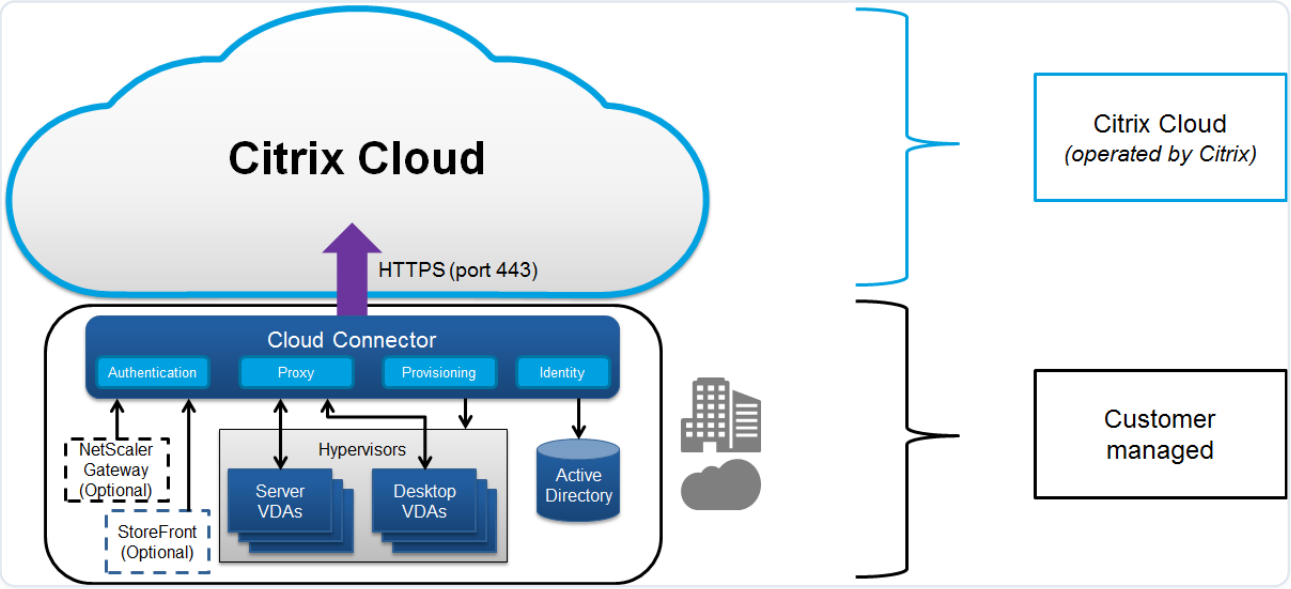
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Technical security overview

Security overview

This document applies to Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) hosted in Citrix Cloud. This information includes Citrix Virtual Apps Essentials and Citrix Virtual Desktops Essentials.

Citrix Cloud manages the operation of the control plane for Citrix DaaS environments. The control plane includes the Delivery Controllers, management consoles, SQL database, license server, and optionally StoreFront™ and Citrix Gateway. The Virtual Delivery Agents (VDAs) hosting the apps and desktops remain under the customer's control in the data center of their choice, either cloud or on-premises. These components are connected to the cloud service using an agent called the Citrix Cloud Connector. If customers elect to use Citrix® StoreFront Cloud, they can also choose to use the Citrix Gateway Service instead of running Citrix Gateway within their data center. The following diagram illustrates Citrix DaaS and its security boundaries.



Citrix cloud-based compliance

Visit the Citrix Trust Center for more information regarding Citrix Cloud Certifications, and check back frequently for updates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The use of Citrix Managed Azure Capacity with various Citrix DaaS™ editions and Universal Hybrid Multi-Cloud has not been evaluated for Citrix SOC 2 (Type 1 or 2), ISO 27001, HIPAA, or other cloud compliance requirements.

Data flow

Citrix DaaS does not host the VDAs, so the customer's application data and images required for provisioning are always hosted in the customer setup. The control plane has access to metadata, such as user names, machine names, and application shortcuts, restricting access to the customer's Intellectual Property from the control plane.

Data flowing between the cloud and customer premises uses secure TLS connections over port 443.

Data isolation

Citrix DaaS stores only the metadata needed for the brokering and monitoring of the customer's applications and desktops. Sensitive information, including images, user profiles, and other application data remains on the customer premises or in their public cloud vendor's subscription.

Service editions

The capabilities of Citrix DaaS vary by edition. For example, Citrix Virtual Apps Essentials™ supports only Citrix Gateway service and Citrix® StoreFront Cloud. Consult that product documentation to learn more about supported features.

ICA® Security

Citrix DaaS provides several options for securing ICA traffic in transit. The following are the options available:

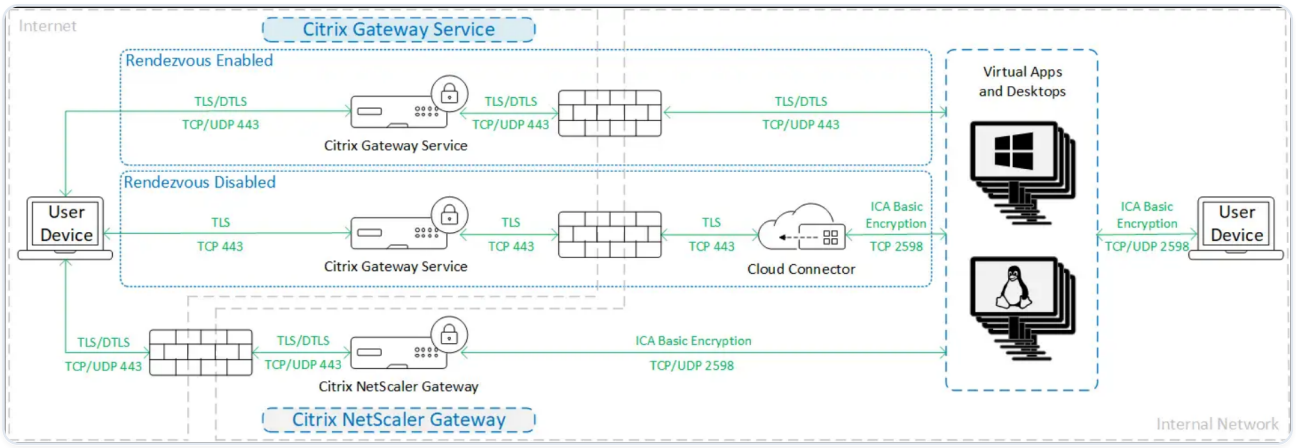
- **Basic encryption:** The default setting.
- **Secure HDX™:** Allows true end-to-end encryption of session data using AES-256.
- **SecureICA:** Allows encrypting session data using RC5 (128-bit) encryption.
- **HDX Direct:** Allows using network-level encryption using TLS/DTLS.
- **VDA TLS/DTLS:** Allows using network-level encryption using TLS/DTLS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Rendezvous protocol:** Available only when using the Citrix Gateway Service. When using the Rendezvous protocol, all segments of the ICA sessions' connections are encrypted using TLS/DTLS.

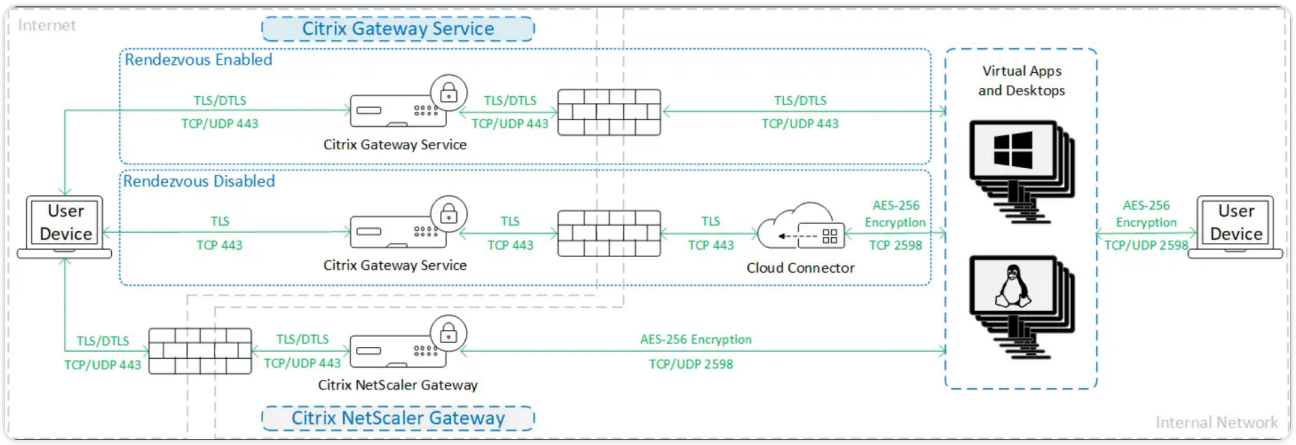
Basic encryption

When using basic encryption, traffic is encrypted as shown in the following diagram.



Secure HDX

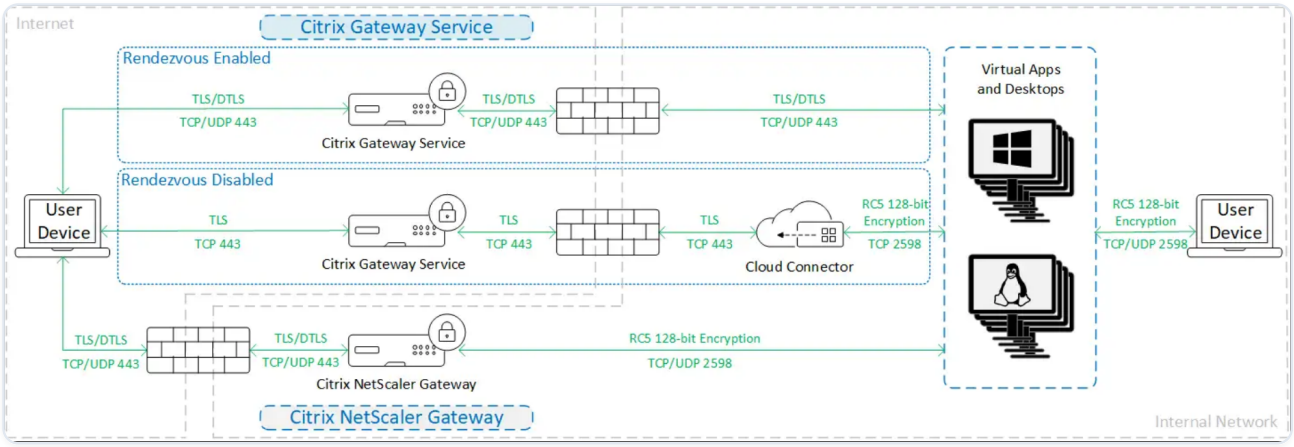
When using Secure HDX, traffic is encrypted as shown in the following diagram.



SecureICA

When using SecureICA, traffic is encrypted as shown in the following diagram.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

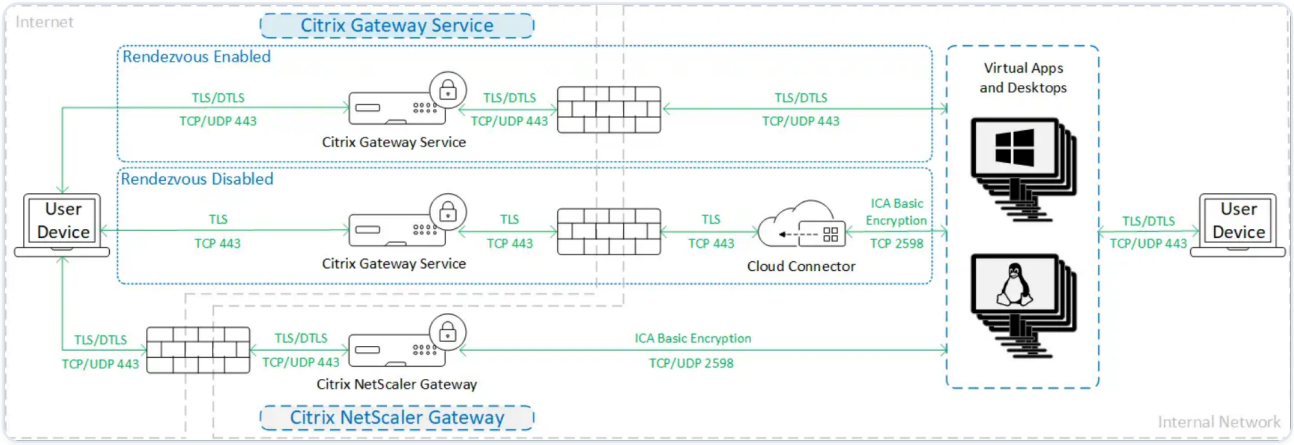
It is recommended to use Secure HDX instead. Secure ICA was deprecated with the release of Citrix Virtual Apps and Desktops 2402.

SecureICA is not supported when using Workspace app for HTML5.

HDX Direct

Internal

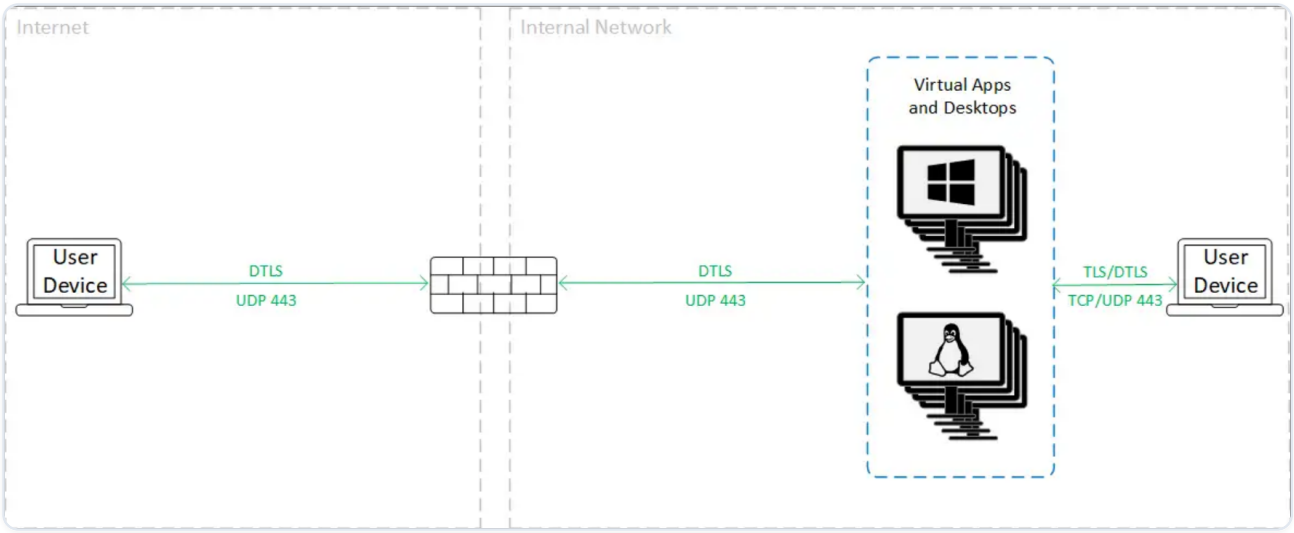
When using HDX Direct in Internal only mode, traffic is encrypted as shown in the following diagram.



External

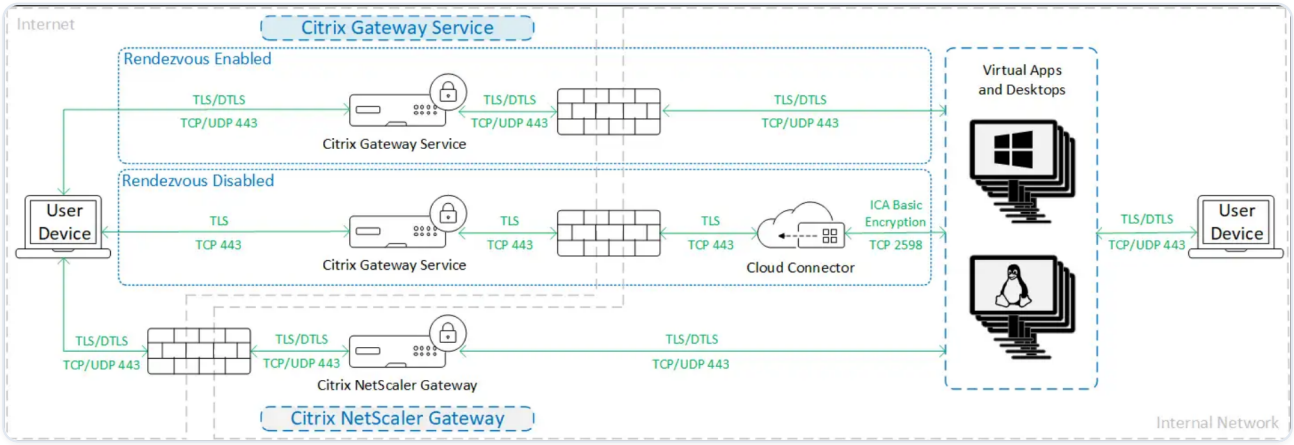
When using HDX Direct in Internal and External mode, traffic is encrypted as shown in the following diagram.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



VDA TLS/DTLS

When using VDA TLS/DTLS encryption, traffic is encrypted as shown in the following diagram.



NOTE:

When using the Gateway Service without Rendezvous, the traffic between the VDA and the Cloud Connector is not TLS encrypted, because the Cloud Connector does not support connecting to the VDA with network-level encryption.

More resources

For more information about the ICA security options and how to configure them, see:

- Secure HDX: Secure HDX
- HDX Direct: HDX Direct
- SecureICA: Security policy settings
- VDA TLS/DTLS: Transport Layer Security

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Rendezvous protocol: Rendezvous protocol

Credential handling

Citrix DaaS handles four types of credentials:

- User Credentials: When end users authenticate using their Active Directory username and password, these are stored to provide single sign on to the VDAs. When using customer-managed StoreFront, these are normally encrypted by the connector before sending to DaaS, for more information see Client access via StoreFront.
- Administrator Credentials: Administrators authenticate against Citrix Cloud. Authentication generates a one-time signed JSON Web Token (JWT) which gives the administrator access to Citrix DaaS.
- Hypervisor Passwords: On-premises hypervisors that require a password for authentication have an administrator-generated password that is directly stored encrypted in the SQL database in the cloud. Citrix manages peer keys to ensure that hypervisor credentials are only available to authenticated processes.
- Active Directory (AD) Credentials: Machine Creation Services™ uses the Cloud Connector for creating machine accounts in a customer's AD. Because the machine account of the Cloud Connector has only read access to AD, the administrator is prompted for credentials for each machine creation or deletion operation. These credentials are stored only in memory, and are held only for a single provisioning event.

Deployment considerations

Citrix recommends that users consult the published best practices documentation for deploying Citrix Gateway applications and VDAs within their environments.

Cloud Connectors

Communication with Citrix Cloud

All connections from Citrix Cloud Connectors to DaaS and other Citrix Cloud services use HTTPS with TLS 1.2.

HTTPS for XML service and STA

If you use on-premise StoreFront or NetScaler Gateways, it is recommended that you enable HTTPS and disable HTTP on the connector. For more information, see HTTPS Configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network access requirements

In addition to the ports described at Inbound and outbound ports configuration, Cloud Connectors have the following network access requirements:

- The Citrix Cloud Connectors require only port 443 outbound traffic to the internet, and can be hosted behind an HTTP proxy.
- Within the internal network, the Cloud Connector needs access to the following for Citrix DaaS:
  - VDAs: Port 80, both inbound and outbound. plus 1494 and 2598 inbound if using Citrix Gateway service
  - StoreFront servers: Port 443 inbound if using HTTPS (recommended) or port 80 if using HTTP (not recommended).
  - Citrix Gateways, if configured as a STA: Port 443 inbound if using HTTPS (recommended) or port 80 if using HTTP (not recommended).
  - Active Directory domain controllers
  - Hypervisors: Outbound only. See Communications Ports Used by Citrix Technologies for specific ports.

Traffic between the VDAs and Cloud Connectors is encrypted using Kerberos message-level security.

Security Keys

You can use Security Keys to ensure that only authorized StoreFront servers and Citrix Gateway appliances are able to connect to DaaS via the cloud connectors. This is especially important if you have enabled XML trust.

Client access

You can provide client access via either Citrix hosted Citrix® StoreFront Cloud or by hosting your own StoreFront deployment.

Users can connect to their store using either Citrix Workspace app or a web browser. For security recommendations for Citrix Workspace app, see the documentation for each platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client access via Citrix® StoreFront Cloud

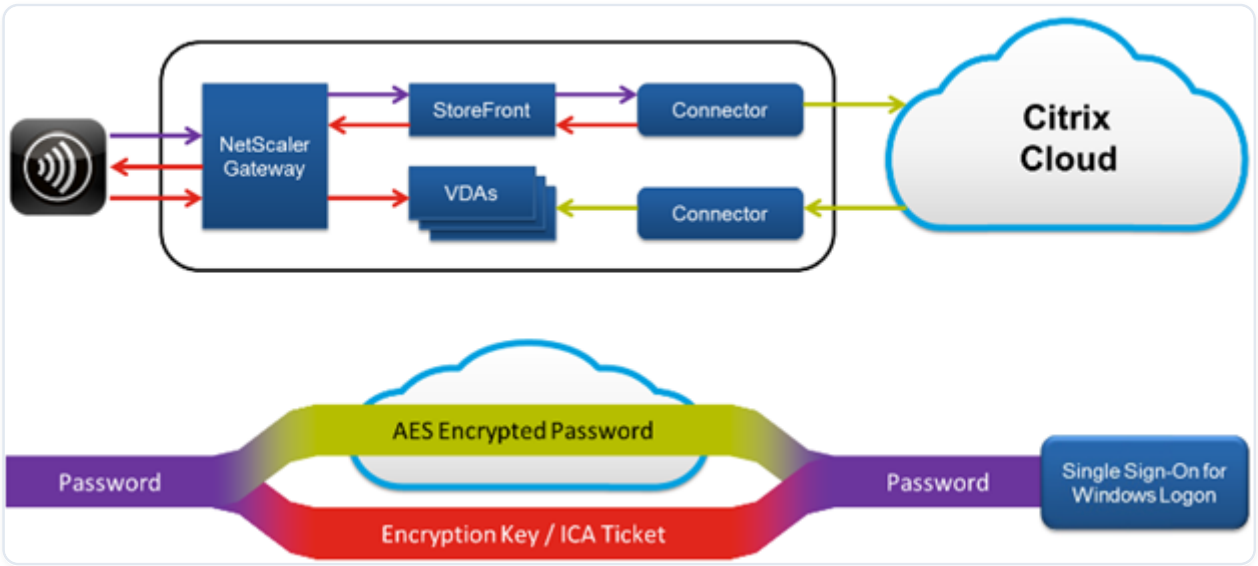
Citrix® StoreFront Cloud is a Citrix managed service that enables client apps to access DaaS resources without needing any on-premises infrastructure. For supported versions of Citrix Workspace app and other requirements, see Citrix® StoreFront Cloud System Requirements. For information on security, see Citrix® StoreFront Cloud security overview.

Client access via Citrix StoreFront

As an alternative to Citrix® StoreFront Cloud, you can provide client access by deploying Citrix® StoreFront in your local environment. This offers greater security configuration options and flexibility for deployment architecture, including the ability to maintain user credentials on-premises. The StoreFront server can be hosted behind a Citrix Gateway to provide secure remote access, enforce multifactor authentication, and add other security features. For more information see Secure your StoreFront deployment.

User credentials

If the user authenticated to StoreFront with their active directory credentials, when a user launches an application, StoreFront passes the credentials to the Cloud Connector. By default the Cloud Connector encrypts user credentials using AES encryption and a random one-time key generated for each launch. The key is never passed into the cloud, and returned only to Citrix Workspace app. The Citrix Workspace app then passes this key to the VDA to decrypt the user password during session launch for a single sign-on experience. The flow is shown in the following figure.



It is important that you configure HTTPS between the client, gateway, storefront and connector to ensure that the password is always encrypted within your network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With the default behavior, as Citrix Cloud does not have access to the credentials, it is unable to forward the credentials to other Cloud Connectors or Connector Appliances for validation. This is required if you use multiple domains without trust relationships. You can disable this behavior and allow credentials to be uploaded to Citrix cloud so that it can forward them to other cloud connectors and Connector Appliances for validation. To configure this use the DaaS PowerShell SDK cmdlet Set-Brokersite with parameter `CredentialForwardingToCloudAllowed`.

Connecting to Cloud Connectors using HTTPS

It is recommended that you configure StoreFront to connect to the Cloud Connectors using HTTPS to ensure all communication is encrypted. This requires that you have enabled HTTPS for XML service and STA. To Configure StoreFront to connect using HTTPS, see Add resource feeds for Citrix Desktops as a Service and Add Citrix Gateway appliance.

XML trust

By default, when StoreFront connects to DaaS for actions such as enumeration and launch, StoreFront must pass through the user's Active Directory credentials so that DaaS can authenticate the user and check the user's group membership. However when using other authentication methods such as domain pass-through, smart cards or SAML, StoreFront does not have the active directory password. In this case you must enable "XML Trust". With XML trust enabled, DaaS allows StoreFront to perform actions on behalf of a user such as enumerating and launching applications without validating the user's password. Before enabling XML trust, use Security Keys or another mechanism such as firewalls or IPsec to ensure that only trusted StoreFront servers are able to connect to the Cloud Connectors.

To enable XML trust in Studio, go to **Settings > Site settings** and turn on **Enable XML trust**.

To use the Citrix DaaS SDK to check the XML trust current value, run Get-BrokerSite and inspect the value of `TrustRequestsSentToTheXMLServicePort`.

To use the Citrix DaaS SDK to enable or disable XML trust, run Set-BrokerSite with parameter `TrustRequestsSentToTheXMLServicePort`.

Citrix Gateway service

Using the Citrix Gateway service avoids the need to deploy Citrix Gateway within customer data centers.

For details, see Citrix Gateway service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

All TLS connections between the Cloud Connector and Citrix Cloud are initiated from the Cloud Connector to the Citrix Cloud. No in-bound firewall port mapping is required.

On-premise NetScaler® gateway

You can use an on-premise NetScaler gateway to provide access to resources. The Gateway must be able to reach cloud connectors to redeem STA tickets. It is recommended you configure the gateway to connect to the Cloud Connectors using HTTPS, see HTTPS for XML service and STA. If you have enabled Security keys then you must configure the gateway to include the keys.

More information

The following resources contain security information:

- Technical security overview for Citrix Managed Azure.
- Citrix Trust Center: The trust center has documentation about standards and certifications that are important in maintaining a secure and compliant IT environment.
- Secure Deployment Guide for the Citrix Cloud Platform: This guide provides an overview of security best practices when using Citrix Cloud and describes the information Citrix Cloud collects and manages. This guide also contains links to comprehensive information about the Citrix Cloud Connector.
- System and Connectivity Requirements.
- Securing Citrix Virtual apps and Desktops on-prem.

NOTE:

This document is intended to provide the reader with an introduction to and overview of the security functionality of Citrix Cloud; and to define the division of responsibility between Citrix and customers with regard to securing the Citrix Cloud deployment. It is not intended to serve as a configuration and administration guidance manual for Citrix Cloud or any of its components or services.

Technical security overview for Citrix Managed Azure

See Technical security overview for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual channel allow list

The virtual channel allow list is a feature that allows you to control which non-Citrix virtual channels are allowed in your environment. By default, the virtual channel allow list feature is enabled. As a result, only Citrix virtual channels are allowed to open in Citrix Virtual Apps and Desktops™ sessions. If there is a need to use custom virtual channels, whether homegrown or from a third party, these need to be explicitly added to the allow list.

Configuration

The virtual channel allow list is enabled by default. You can configure this feature using the following settings in the Citrix policy:

- **Virtual channel allow list**: to enable or disable the feature and to add virtual channels to the list.
- **Virtual channel allow list log throttling**: sets the throttling period for the virtual channel allow list event logging.
- **Virtual channel allow list logging**: sets the logging level for the virtual channel allow list.

Adding virtual channels to the allow list

To add a virtual channel to the allow list, you need the following information:

1. The virtual channel name as defined in the code, which can be up to seven characters long. For example, `CTXCVC1`.
2. The paths to the processes that open the virtual channel on the VDA machine. For example, `C:\Program Files\Application\run.exe`.

Once you have the required information, you must add the virtual channel to the allow list using the Virtual channel allow list policy setting. To add a virtual channel to the list, enter the virtual channel name followed by a comma, and then the path to the process that accesses the virtual channel. If there are multiple processes, you can add these processes by separating each process with commas.

For single processes

Using the previous examples, add the following entry to the list:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For multiple processes

If there are multiple processes, add the following entry to the list:

`CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe`

Using wildcards

The use of wildcards (*) is supported. You can use wildcards when the names of directories or executables change based on the version of the application, or if the third-party component is installed in the users' profiles.

You can use wildcards in the following scenarios:

- To replace the full directory name. For example: `C:\Program Files\Application*\run1.exe`
- To replace part of the directory name. For example: `C:\Program Files\Application\v*\run1.exe`
- To replace the executable's name. For example: `C:\Program Files\Application\v1.2*.exe`
- To replace part of the executable's name. For example: `C:\Program Files\Application\v1.2\run*.exe`

The following restrictions apply:

- The wildcard can only be used to replace a single directory. For example, if the executable is located in `C:\Program Files\Application\v1.2\run1.exe`
  - Allowed: `C:\Program Files\Application*\run1.exe`
  - Not allowed: `C:\Program Files*\run1.exe`
- Entries must contain the file name extension.
  - Allowed: `C:\Program Files\Application\v1.2*.exe`
  - Not allowed: `C:\Program Files\Application\v1.2*`
- All paths must be local.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Network paths are not allowed.
- Wildcard support is available from Citrix Virtual Apps and Desktops 2206.
- Wildcard support is available in Citrix Virtual Apps and Desktops 2203 LTSR from CU2.

Using system environment variables

You can use system environment variables to simplify the definition of the trusted processes in your allow list. You can use any of the out-of-box variables, such as `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%`, and `%systemroot%`.

You can also use custom environment variables as long as they are defined at the system level.

The following examples depict out-of-box environment variables:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

The following example depicts a custom system environment variable:

- Custom variable name: `app`
- Custom variable value: `%programfiles%\Application\`
- Allow list entry: `CTXCVC1,%app%\run.exe`

NOTE:

User environment variables are not supported.

Environment variable support is available from Citrix Virtual Apps and Desktops version 2209.

Obtain virtual channel names and processes

The easiest way to obtain the name of the virtual channel and the process that opens it on the VDA machine is to get the information from the developer or a third-party vendor that provided the virtual channel.

Alternatively, you can obtain information by applying the feature's logs and following these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Once the client and server components of the custom virtual channel are in place, launch a virtual application or virtual desktop.
2. In the VDA machine's System event log, look for the custom virtual channel's name and the process that tried to open it. For more information on available events, see Event logs.
3. Log out from the session.
4. Add an entry in the virtual channel allow list policy settings for the identified virtual channel and process.
5. Restart the machine.
6. Once the VDA is registered, run the virtual application or virtual desktop to validate that the custom virtual channels open successfully.

Considerations for Citrix virtual channels

All built-in Citrix virtual channels are trusted and allowed to open without further configuration. However, the following two features require explicit entries in the allow list because of external dependencies:

- Multimedia Redirection
- HDX RealTime Optimization Pack for Skype for Business

Multimedia Redirection

If you use a media player other than Windows Media Player as your system media player, you need to add it to the allow list as a trusted process. The following information is required for the allow list entry:

- Virtual channel name: `CTXMM`
- Process: Path to the media player used in your VDA machine. For example, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Allow list entry: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack for Skype for Business

The following information is required for the allow list entry:

- Virtual channel name: `CTXRMEP`
- Process: Path to the Skype for Business executable in your VDA machine, which can vary based on the version of Skype for Business or if you used a custom installation path. For example, `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Allow list entry: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Delivery methods

A single delivery method likely cannot meet all of your requirements.

You can consider several application delivery methods. Choosing the appropriate method helps improve scalability, management, and user experience.

- **Installed app:** The application is part of the base desktop image. The install process involves dll, exe, and other files copied to the image drive in addition to registry modifications. For details, see Create machine catalogs.
- **Streamed app (Microsoft App-V):** The application is profiled and delivered to the desktops across the network on-demand. Application files and registry settings are placed in a container on the virtual desktop, isolated from the base operating system and each other. This action helps address compatibility issues. For details, see App-V.
- **Layered app (Citrix App Layering):** Each layer contains a single application, agent, or operating system. By integrating one OS layer, one platform layer (for example, VDA) and many application layers, an administrator can easily create new, deployable images. Layering simplifies ongoing maintenance, as an OS, agent and application exists in a single layer. When you update the layer, all deployed images containing that layer are updated. See Citrix App Layering.
- **Hosted Windows app:** An application installed on a multi-user Citrix Virtual Apps host and deployed as an application and not a desktop. A user accesses the hosted Windows app seamlessly from the VDI desktop or endpoint device, hiding the fact that the app is running remotely. For details, see Create delivery groups.
- **Local app:** An application deployed on the endpoint device. The application interface appears within the user's hosted VDI session even though it runs on the endpoint. For details, see Local App Access and URL redirection.

For desktops, you can consider Citrix Virtual Apps™ published desktops or VDI desktops.

Citrix Virtual Apps published apps and desktops

Use multi-session OS machines to deliver Citrix Virtual Apps published apps and published desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use case:

- You want inexpensive server-based delivery to minimize the cost of delivering applications to many users, while providing a secure, high-definition user experience.
- Your users perform well-defined tasks and do not require personalization or offline access to applications. Users can include task workers such as call center operators and retail workers, or users that share workstations.
- Application types: any application.

Benefits and considerations:

- Manageable and scalable solution within your data center.
- Most cost effective application delivery solution.
- Hosted applications are managed centrally and users cannot modify the application, providing a user experience that is consistent, safe, and reliable.
- Users must be online to access their applications.

User experience:

- User requests one or more applications from StoreFront™, their Start menu, or a URL you provide to them.
- Applications are delivered virtually and display seamlessly in high definition on user devices.
- Depending on profile settings, user changes are saved when the user's application session ends. Otherwise, the changes are deleted.

Process, host, and deliver applications:

- Application processing takes place on hosting machines, rather than on the user devices. The hosting machine can be a physical or a virtual machine.
- Applications and desktops reside on a multi-session OS machine.
- Machines become available through machine catalogs.
- Machines from machine catalogs are organized into delivery groups that deliver the same set of applications to groups of users.
- Multi-session OS machines support delivery groups that host either desktops or applications, or both.

Session management and assignment:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Multi-session OS machines run multiple sessions from a single machine to deliver multiple applications and desktops to multiple, simultaneously connected users. Each user requires a single session from which they can run all their hosted applications.

  For example, a user logs on and requests an application. One session on that machine becomes unavailable to other users. A second user logs on and requests an application which that machine hosts. A second session on the same machine is now unavailable. If both users request more applications, no additional sessions are required because a user can run multiple applications using the same session. If two more users log on and request desktops, and two sessions are available on that machine, that one machine now uses four sessions to host four different users.
- Within the delivery group to which a user is assigned, a machine on the least loaded server is selected. A machine with session availability is randomly assigned to deliver applications to a user when that user logs on.

VM hosted apps

Use single-session OS machines to deliver VM hosted applications

Use case:

- You want a client-based application delivery solution that is secure, provides centralized management, and supports many users per host server. You want to provide those users with applications that display seamlessly in high-definition.
- Your users are internal, external contractors, third-party collaborators, and other provisional team members. Your users do not require offline access to hosted applications.
- Application types: Applications that might not work well with other applications or might interact with the operation system, such as Microsoft .NET framework. These types of applications are ideal for hosting on virtual machines.

Benefits and considerations:

- Applications and desktops on the image are securely managed, hosted, and run on machines within your data center, providing a more cost effective application delivery solution.
- Upon logon, users can be randomly assigned to a machine within a delivery group that is configured to host the same application. You can also statically assign a single machine to deliver an application to a single user each time that user logs on. Statically assigned machines allow users to install and manage their own applications on the virtual machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Running multiple sessions is not supported on single-session OS machines. Therefore, each user consumes a single machine within a delivery group when they log on, and users must be online to access their applications.
- This method can increase the amount of server resources for processing applications and increase the amount of storage for users' personal vDisks.

User experience:

- The same seamless application experience as hosting shared applications on multi-session OS machines.

Process, host, and deliver applications:

- The same as multi-session OS machines except they are virtual single-session OS machines.

Session management and assignment:

- Single-session OS machines run a single desktop session from a single machine. When accessing applications only, one user can use multiple applications (and is not limited to a single application). The operating system sees each application as a new session.
- Within a delivery group, logged-on users can access either a statically assigned machine (each time the user logs on to the same machine), or a randomly assigned machine that is selected based on session availability.

VDI desktops

Use single-session OS machines to deliver Citrix Virtual Desktops™ VDI desktops.

VDI desktops are hosted on virtual machines and provide each user with a desktop operating system.

VDI desktops require more resources than Citrix Virtual Apps published desktops, but do not require that applications installed on them support server-based operating systems. Also, depending on the type of VDI desktop you choose, these desktops can be assigned to individual users. This allows users a high level of personalization.

When you create a machine catalog for VDI desktops, you create one of these types of desktops:

- **Random non-persistent desktop, also known as pooled VDI desktop:** Each time a user logs on to one of these desktops, that user connects to a desktop selected from a pool of desktops. That pool is based on a single image. All changes to the desktop are lost when the machine restarts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Static non-persistent desktop:** During the first logon, a user is assigned a desktop from a pool of desktops. (Each machine in the pool is based on a single image.) After the first use, each time a user logs on to use one of these desktops, that user connects to the same desktop that was assigned on first use. All changes to the desktop are lost when the machine restarts.
- **Static persistent desktop:** Unlike other types of VDI desktops, users can fully personalize these desktops. During the first logon, a user is assigned a desktop from a pool of desktops. Subsequent logons from that user connect to the same desktop that was assigned on first use. Changes to the desktop are retained when the machine restarts.

Remote PC Access

Remote PC Access is a feature of Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) that enables organizations to easily allow their employees to access corporate resources remotely in a secure manner. The Citrix platform makes this secure access possible by giving users access to their physical office PCs. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Remote PC Access eliminates the need to introduce and provide other tools to accommodate teleworking. For example, virtual desktops or applications and their associated infrastructure.

Remote PC Access uses the same Citrix DaaS™ components that deliver virtual desktops and applications. As a result, the requirements and process of deploying and configuring Remote PC Access are the same as those required for deploying Citrix DaaS for the delivery of virtual resources. This uniformity provides a consistent and unified administrative experience. Users receive the best user experience by using Citrix HDX to deliver their office PC session.

For more information, Remote PC Access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Plan and build a deployment

If you're not familiar with the components, terminology, and objects used with Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), see Citrix DaaS.

If you're migrating from a Citrix Virtual Apps and Desktops deployment, see Migrate to cloud.

IMPORTANT:

To ensure that you get important information about Citrix Cloud™ and the Citrix services you subscribe to, make sure you can receive all email notifications.

In the upper right corner of the Citrix Cloud console, expand the menu to the right of the customer name and OrgID fields. Select **Account Settings**. On the **My Profile** tab, select all entries in the **Email Notifications** section.

How to use this article

To set up your Citrix DaaS™ deployment, complete the tasks summarized below. Links are provided to each task's details.

Review the entire process before starting the deployment, so you know what to expect. This article also links to other helpful information sources.

NOTE:

If you plan to use the Quick Deploy workflow to provision Microsoft Azure machines, follow the setup guidance in Get started with Quick Deploy.

Plan and prepare

In the Citrix Tech Zone documentation, see a step-by-step proof of concept guide for this service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sign up

Sign up for a Citrix account and request a Citrix DaaS demo.

Set up a resource location

A resource location contains resources required to deliver applications and desktops to users. Creating resource locations enables DaaS to use those resources. To learn more about resource locations, see Connect to Citrix Cloud.

Before creating machines, you must connect a resource location to DaaS:

- Domain-joined machines require that you have Cloud Connectors installed in the resource location. In this case, you can create:
  - Identity pool of on-premises Active Directory joined machine identity
  - Identity pool of Microsoft Entra joined machine identity
  - Identity pool of Microsoft Entra hybrid joined machine identity

  For high availability, we recommend that you install two Cloud Connectors in each resource location. See Cloud Connector installation.

  More information:

  - What are resource locations and Cloud Connectors?
  - Video about installing Cloud Connectors:

    
- Non-domain-joined machines don’t require Cloud Connectors but require that you have Rendezvous V2 enabled. The Rendezvous protocol allows VDAs to bypass the Cloud Connectors to connect directly and securely with DaaS. See Rendezvous V2. In this case, you can:
  - Identity pool of non-domain-joined machine identity

If you're using the Quick Deploy interface to provision Azure VMs, Citrix creates the resource location and Cloud Connectors for you.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a connection to the resource location

After you add a resource location and Cloud Connectors, create a connection to the resource location using Studio.

This step isn't necessary in either of the following cases:

- You're building a simple proof of concept deployment
- You're using the Quick Deploy interface to provision Azure VMs.

More information:

- What are hosts?
- What are host connections?

Install VDAs

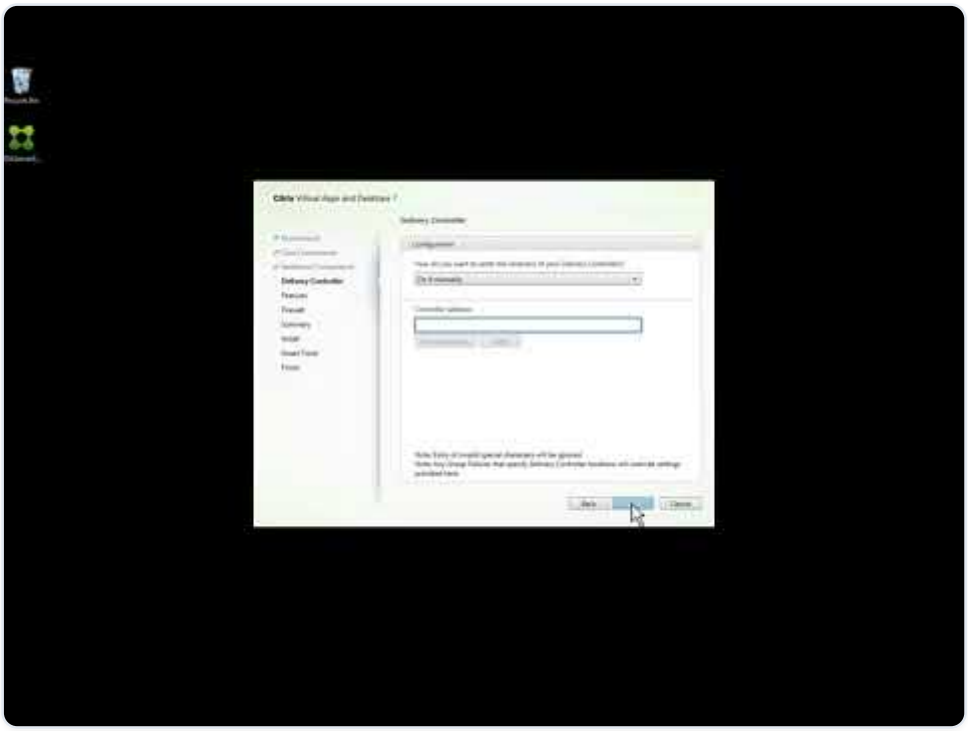
Each machine that delivers applications and desktops to users must have a Citrix Virtual Delivery Agent (VDA) installed on it.

- For a simple proof of concept deployment, download and install a VDA on one machine.
- If you're using an image to provision VMs, install a VDA on the image.
- For a Remote PC Access deployment, install the core version of the VDA for single-session OS on each physical office PC.

How-to and more information:

- What are VDAs?
- Installation preparation and instruction
- Command-line VDA installation
- Video about downloading and installing a VDA:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



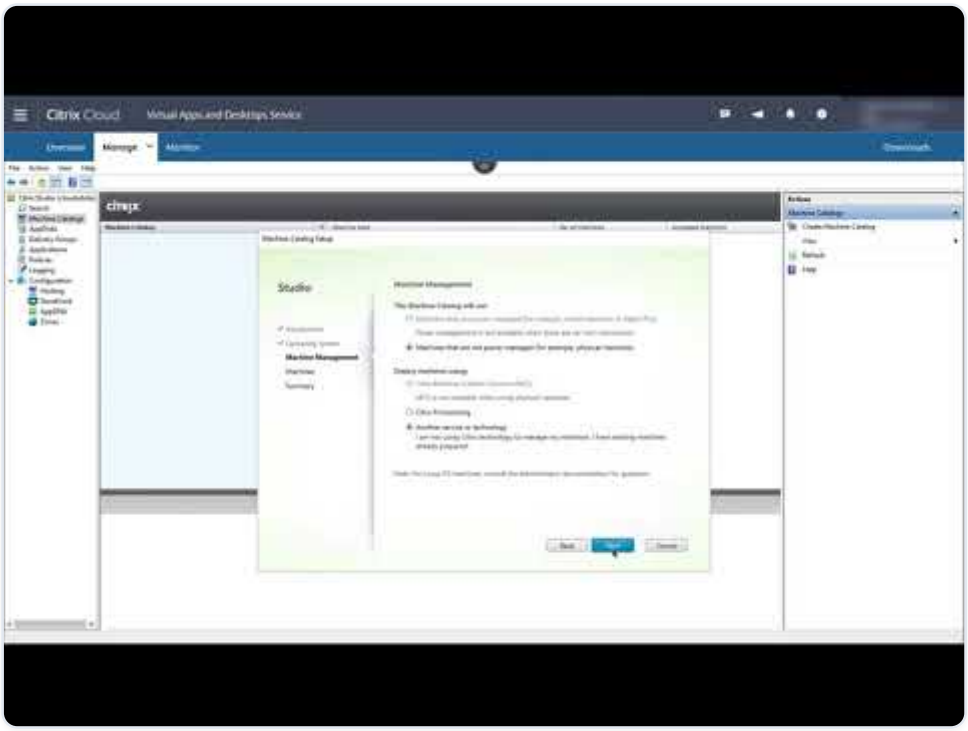
Create a catalog

After you create a connection to your resource location (if needed), you create a catalog. If you're using Studio, the workflow guides you automatically to this step.

How-to and more information:

- What are catalogs?
- Create a catalog
- Use the Quick Deploy interface to deploy a catalog containing Azure VMs.
- Video about creating a catalog using Studio:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create a delivery group

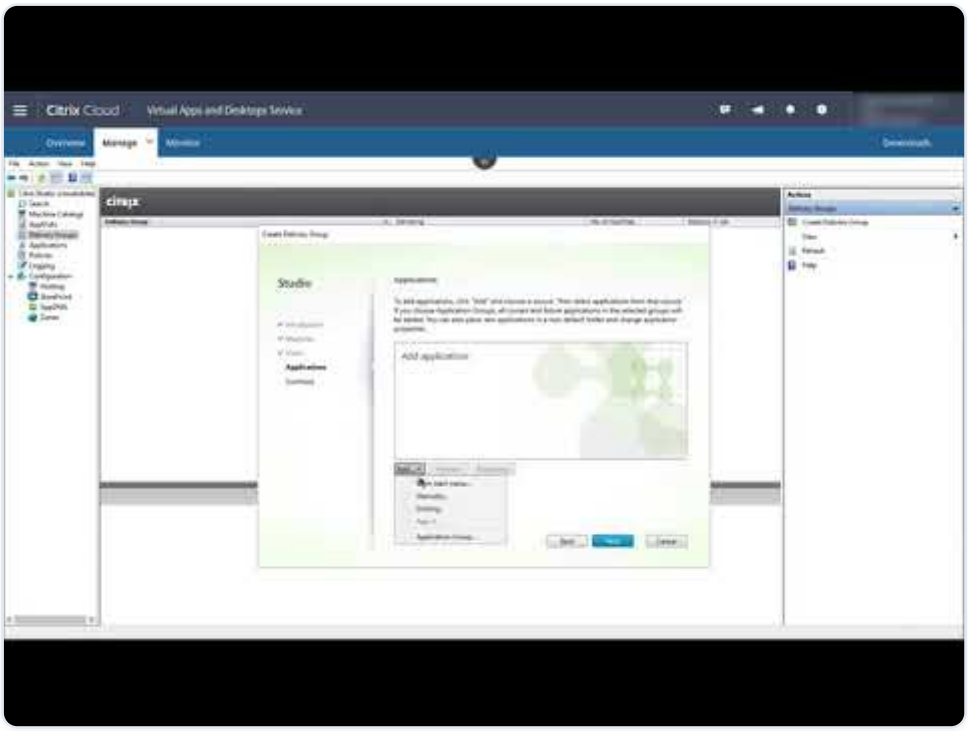
After you create your first catalog, the **Manage** workflow guides you to create a delivery group.

This step isn't necessary if you're using the Quick Deploy interface to provision Azure VMs.

How-to and more information:

- What are delivery groups?
- Create a delivery group
- Video about how to create a delivery group:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Deploy other components and technologies

After you complete the tasks above that set up the Citrix DaaS deployment, you'll find information about provisioning and configuring other components and technologies in the Citrix solution, such as:

- Citrix policies
- StoreFront
- App Layering
- Workspace Environment Management (WEM) Service
- Citrix Gateway service
- Zones
- Federated Authentication Service (FAS)

Complete other tasks that apply to your configuration. For example, if you plan to deliver Windows Server workloads, configure a Microsoft RDS License Server.

Launch applications and desktops

After you configure your deployment, publishing occurs automatically. Applications and desktops that you configured are available to users in their stores. A user simply navigates to their store URL and selects an application or desktop, which launches immediately.

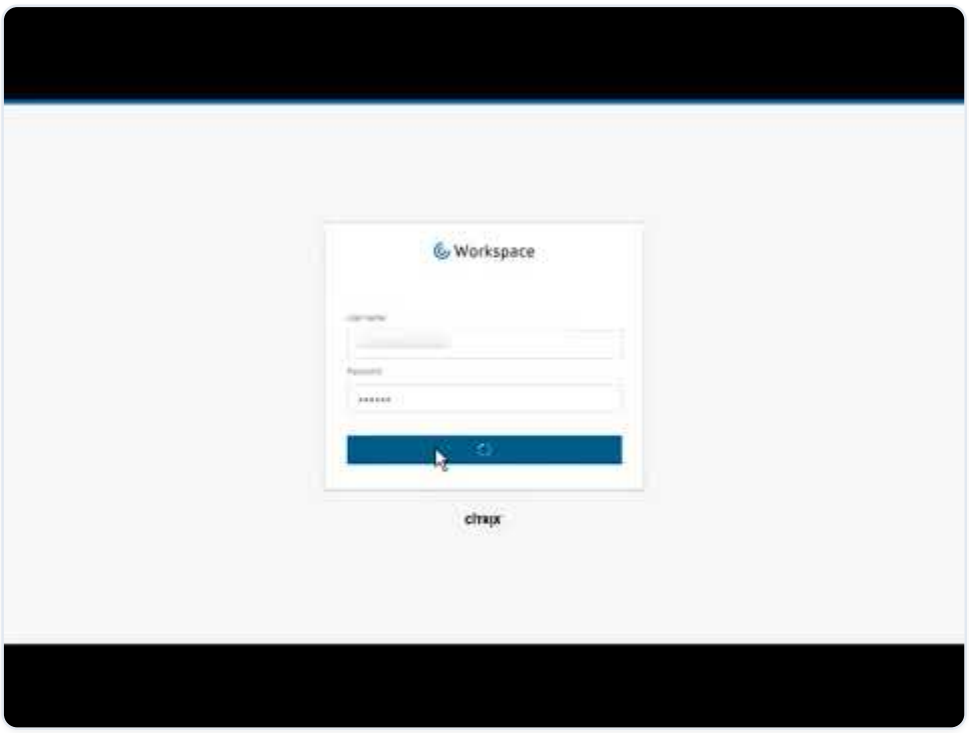
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Send the store URL to your users. You can find the store URL in two locations:

- From the Citrix Cloud console, select **StoreFront Cloud** from the menu in the upper left corner. The **Access** tab contains the store URL.
- From the Citrix DaaS **Overview** page, the store URL appears near the bottom of the page.

More information:

- Video about users launching applications and desktops from their stores:



More information

The Citrix Cloud Learning series provides education courses that are organized by your path:

- If you're new to Citrix DaaS, see New to Citrix DaaS Learning Path.
- If you're migrating from a Citrix Virtual Apps and Desktops deployment, see Migrating Citrix Virtual Apps and Desktops to Citrix Cloud Learning Path.

Sign up for Citrix DaaS™

Introduction

You can subscribe to Citrix DaaS through Citrix or through the Azure Marketplace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you plan to use Citrix Managed Azure, you can also order the Citrix Azure Consumption Fund through Citrix or through the Azure Marketplace.

- When you order through Citrix, you can order Citrix DaaS and the Citrix Azure Consumption Fund at the same time.
- When you order through Azure Marketplace, you first order Citrix DaaS. Then, you can place another order for the Citrix Azure Consumption Fund.

If you order only Citrix DaaS now, you can order the Citrix Azure Consumption Fund later, either through Azure Marketplace or your Citrix account representative.

Demos and trials

You can evaluate Citrix DaaS by request through Citrix. From a trial, you can convert to a paid service subscription.

During a trial, you can optionally use a Citrix Managed Azure subscription for catalogs, images, and network connections. If you have Citrix-managed resources at the time you convert to a paid subscription, you must either purchase consumption or delete those Citrix-managed resources. If you do not purchase consumption, those resources are deleted automatically, which might affect users.

If you currently subscribe to a Citrix DaaS service

Generally, a Citrix Cloud™ account allows you to subscribe to only one of Citrix DaaS's services (or one edition) at a time per Citrix OrgID. For example, you can subscribe to Citrix DaaS Premium edition OR Citrix DaaS for Azure, but not both.

If you currently subscribe to a Citrix DaaS, and want to subscribe to this service, you have two choices:

- Subscribe to this service using a different Citrix Cloud account (OrgID).
- Decommission Citrix DaaS you already have, and then order this service. For decommission instruction, see CTX239027.

Order through Citrix

You can order this service (and the Citrix Azure Consumption Fund) through Citrix Cloud or through your Citrix account representative.

Through Citrix Cloud:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Follow the guidance in Sign up for Citrix Cloud to get a Citrix Cloud account and Organization ID.
- You can request a Citrix DaaS demo. In the Citrix DaaS tile, click **Request Demo**. Provide the requested information.

  A Citrix representative will contact you to discuss your requirements, environment, and plans. Depending on our representative's assessment, you will be authorized to participate in an administrator demo or a proof of concept trial. For more information, see Citrix Cloud Service Trials.

When you are authorized for a trial, the text on Citrix DaaS tile in the Citrix Cloud console changes to **Manage**.

Order through Azure Marketplace

You can order the following Citrix offerings through Azure Marketplace:

- Citrix DaaS for Azure
- Citrix DaaS Advanced edition
- Citrix DaaS Premium edition
- Workspace Premium Plus

If you plan to host your Citrix Virtual Apps and Desktops workloads on Microsoft Azure, and want to use a Citrix Managed Azure subscription, order the Citrix Azure Consumption Fund after ordering Citrix DaaS or Workspace Premium Plus.

With the Citrix Azure Consumption Fund, you're charged each month for your consumption, which can vary depending on the hosting resources you choose and the hours of use. You can review your consumption use through Citrix Cloud.

From the Azure Marketplace:

- You cannot combine Citrix DaaS and consumption fund in one order.
- The order process for the Citrix Azure Consumption Fund is essentially the same as ordering Citrix DaaS, but you must have previously ordered Citrix DaaS.

Requirements for ordering through Azure Marketplace

- The OrgID of your Citrix Cloud account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - If you have a Citrix Cloud account, but don't know the OrgID, look in the upper right corner of the Citrix Cloud console. Or, look at the email you received when you created the account.
  - If you don't have a Citrix Cloud account, follow the guidance in Sign up for Citrix Cloud.

- An Azure account and at least one Azure subscription in that account.

Procedure for ordering through Azure Marketplace

Follow this procedure to order a Citrix DaaS or Workspace Premium Plus through Azure Marketplace. (If you want to use Citrix Managed Azure, place another order for the Citrix Azure Consumption Fund, after you order Citrix DaaS.)

1. Sign in to the Azure Marketplace using your Azure account credentials.
2. Search for and then navigate to the Citrix offering you want to order.
3. Select **Get it now**.
4. On the **One more thing** message, fill in the required information, enable the consent check box, and then select **Continue**.
5. Review the tabs containing information about the product, plans, pricing, and usage. When you're ready, select a plan (if more than one is available), and then select **Set up + subscribe**.
6. On the **Basics** tab:
   - **Subscription:** Indicates the plan that you selected.
   - **Resource group:** Select or create a resource group.
   - **Name:** Enter a name for your subscription order so you can easily identify it later.
   - The **Plan** information shows the price for the selected plan, based on the billing term. To change the plan term, select **Change plan**. Select the term you want and select **Change plan**.
7. On the **Review + subscribe** tab, review the contact information, and update it, if needed. Review the basic subscription information. Select **Subscribe**.
8. On the **Subscription in progress** page, select **Configure account now**. (If the button is disabled, wait a moment.) You're taken to a Citrix activation page.
9. On the activation page:
   - Use the **Sign in** link to sign in to Citrix Cloud. A successful sign-in automatically populates the **Organization ID** field.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Quantity:** Enter the number of users. (An initial order must be at least 25.) An estimated price is displayed.
- Agree to the terms and conditions, and then select **Activate Order**.

After ordering through Azure Marketplace

Citrix sends you an email when your service is provisioned. Provisioning can take a while. If you don't receive the email by the following day, contact Citrix Support. When you receive the email from Citrix, you can begin using Citrix DaaS.

Fulfillment of a Citrix Azure Consumption Fund order does not take much time. When Citrix is notified of the order, a banner appears in the Citrix DaaS console, indicating that a Citrix Managed Azure subscription will be prepared for you.

Do not delete Citrix DaaS resource in Azure. Deleting that resource cancels your subscription.

Order through Google Cloud Marketplace

You can order the following Citrix offerings through Google Cloud Marketplace:

- Citrix DaaS Standard for Google Cloud
- Citrix DaaS Premium for Google Cloud

You need the following to order through Google Cloud Marketplace:

- The OrgID of your Citrix Cloud account.
  - If you have a Citrix Cloud account, but don't know the OrgID, look in the upper right corner of the Citrix Cloud console. Or, look at the email you received when you created the account.
  - If you don't have a Citrix Cloud account, follow the guidance in Sign up for Citrix Cloud.
- A Google Cloud account and at least one Google Cloud subscription in that account.

To place your order:

1. Sign in to Google Cloud Marketplace
2. Follow the instructions on the Citrix DaaS for Google Cloud page to make your purchase.

Citrix sends you an email when your service is provisioned. Provisioning can take a while. If you don't receive the email by the following day, contact Citrix Support. When you receive the email from Citrix, you can begin using Citrix DaaS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Do not delete Citrix DaaS resource in Google Cloud. Deleting that resource cancels your subscription.

What's next

After your order is fulfilled, continue with the next steps in Plan and build a deployment.

For example:

- If you haven't already set up your hypervisor or cloud service, or Active Directory, see Set up a resource location.
- If your host environment and Active Directory are already set up, see Create a connection.

Citrix DaaS™ for Microsoft Azure

With Studio, you can deploy and manage virtual apps and desktops on Microsoft Azure. Detailed steps are as follows:

1. Sign in to Citrix Cloud.
2. Click on the **DaaS** tile to open Studio.
3. Deploy virtual apps and desktops using one of these workflows:

    - **Quick Deploy > Microsoft Azure** (recommended for fast, guided deployment). For more information, see Quick Deploy for Microsoft Azure.

      NOTE:

      To perform advanced configurations or management options for your deployment, use the Studio related nodes. For more information see Studio.

    - **Studio** (recommended for advanced configuration requirements). For more information, see Get started: Plan and build a deployment.

For more information about the difference between the Quick Deploy and the Studio workflows, see the following section.

Quick Deploy for Microsoft Azure

In Studio, the **Quick Deploy > Microsoft Azure** interface offers fast deployment of apps and desktops when you're using Microsoft Azure to host your desktops and apps. This interface offers *basic* configuration, *without* advanced features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With Quick Deploy, you can:

- Provision virtual machines and catalogs that deliver desktops and apps hosted in Microsoft Azure.
- Create Remote PC Access catalogs for existing machines.

For more information, see Citrix DaaS Standard for Azure.

NOTE:

With Quick Deploy, you can use a Citrix-Managed Azure subscription, or your own Azure subscription.

Differences between Quick Deploy and Studio workflows

As an alternative to Quick Deploy, the Studio workflow offers advanced configuration features. See the following table for details.

FEATURE	QUICK DEPLOY	STUDIO
Deploy using Azure	Yes	Yes *
Citrix® prepared images available	Yes	No
Simplified user experience	Yes	No

* When using a Citrix Managed Azure subscription, you must use Quick Deploy when creating an image or catalog.

If you're familiar with using the Studio workflow to create and manage catalogs, Quick Deploy has the following differences:

- Different terminology.
  - In Quick Deploy, you create a catalog.
  - In Machine Catalogs, you create a machine catalog. In practice, it's often referred to as simply catalog.
- Resource location and Cloud Connectors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Quick Deploy automatically creates a resource location including two Cloud Connectors when you create your first catalog.
    - In the Studio workflow, creating a resource location and adding Cloud Connectors are separate steps that you must complete in Citrix Cloud before creating a catalog.

- Images used to create catalogs.

    - Quick Deploy offers several Citrix prepared images of Windows and Linux machines. You can use these images to create catalogs.

      You can also use these images to create images and then customize the new images to suit your unique deployment needs. This feature is known as the image builder. You can also import images from your own Azure subscription.
    - In the Studio workflow, you customize images from the supported host you're using. Citrix prepared images are not available.

- Catalog displays:

    - Catalogs created in Quick Deploy are visible in the Quick Deploy and the Studio section displays.
    - Catalogs created in the Studio workflow are not visible in the Quick Deploy display.

- Delivery groups:

    - You do not create delivery groups in Quick Deploy. In Quick Deploy, you specify the machines, applications, desktops, and users (subscribers) in the catalog.

      Citrix automatically creates a delivery group for each Quick Deploy catalog, using the same name as the catalog. That action occurs behind the scenes. You don’t need to do anything to create the delivery group. The delivery group appears only in the Delivery Groups node, not in Quick Deploy.
    - In the Studio workflow, you create a delivery group and indicate which machines it contains. Optionally, you also specify applications, desktops, and users. You can also create application groups.

- Layout and user interface.

    - The Quick Deploy interface has a different layout and style from the Studio workflow. Quick Deploy contains more on-screen guidance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The interfaces aren't mutually exclusive. You can use Quick Deploy to create some catalogs, and then use the Machine Catalogs node to create other catalogs.

Citrix HDX™ Plus for Windows 365

Citrix HDX Plus for Windows 365 allows you to integrate Citrix Cloud™ with Windows 365 to use Citrix HDX technologies for an enhanced and more secure Windows 365 Cloud PC experience in addition to other Citrix Cloud services for enhanced manageability.

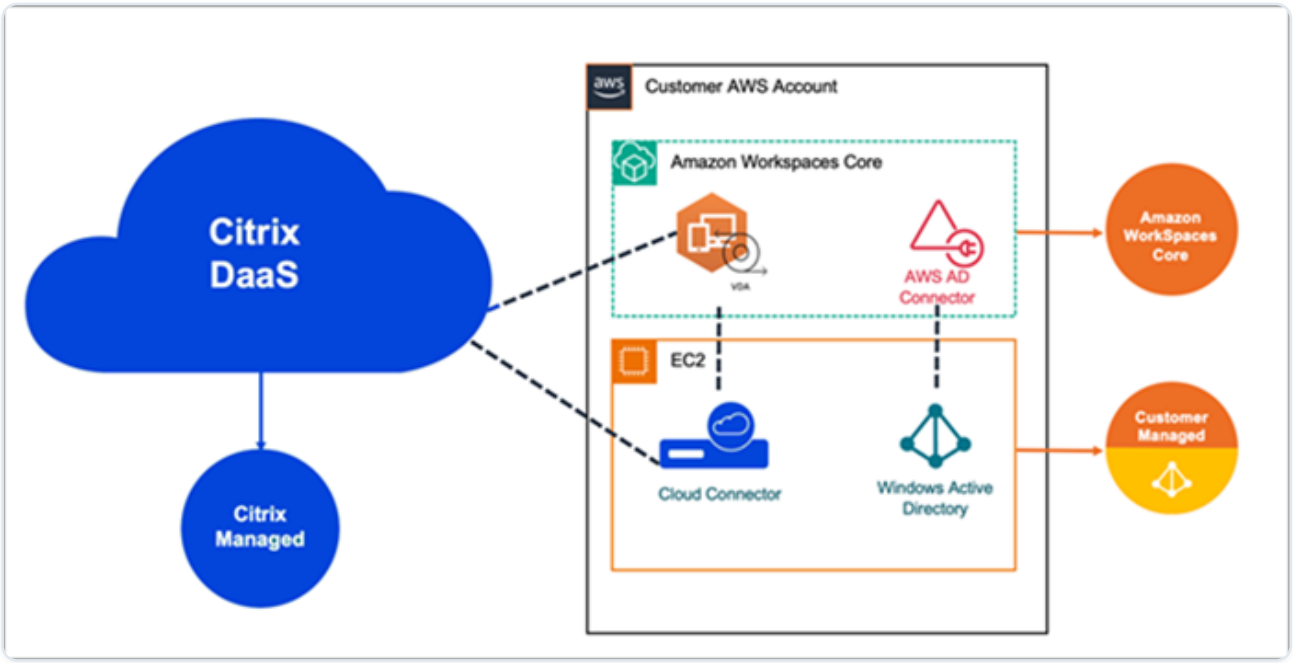
For more information, see Citrix HDX Plus for Windows 365

Citrix DaaS™ Quick Deploy for Amazon WorkSpaces Core Bundles

Introduction

This article describes how to prepare and create a deployment with Citrix® for Amazon WorkSpaces Core. Amazon WorkSpaces Core resides in Amazon Web Services (AWS).

The following is the representation of the AWS implementation and its management with Citrix DaaS:



Prepare and create a deployment

The deployment checklist in the **Quick Deploy** interface contains links to procedures 1-6.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Before you start, complete the prerequisites in Citrix Cloud and AWS.
2. Create a resource location in Citrix Cloud. (This procedure is also included as a prerequisite.)
3. Connect your AWS account. This procedure enables permissions so that the Citrix DaaS can connect to AWS.
4. Create a directory connection. This procedure configures a connection that allows access to your organization's Active Directory.
5. Import an image. This procedure enables you to create a desktop experience for your users.
6. Create a deployment. This procedure specifies the machines to be deployed and the users who can access them through their store.

Before you start

Make sure you've completed the following tasks before you begin preparing and creating your deployment.

There is one exception: Creating a resource location in Citrix Cloud is listed as a prerequisite. It is also the first procedure in the deployment checklist. So, if you create the resource location as part of the prerequisites, skip that procedure in the checklist sequence. Similarly, complete that procedure in the checklist if you didn't do it earlier.

Prerequisites to complete in Citrix Cloud

- Create a Citrix Cloud account and subscribe to the Citrix DaaS.
- Create a Citrix Cloud resource location. (This procedure is also linked in the Quick Deploy interface.)

Prerequisites to complete in AWS

- Create an AWS user account. The account must have:
  - Role permissions for the Citrix API client.
  - Permissions for programmatic access. For more information, see AWS account programmatic access permissions.
  - Create the workspaces_DefaultRole role. For more information, see Create the workspaces_DefaultRole Role.
- In your Active Directory:
  - Use the AD Connector option to store and manage information. For more details, see AD Connector.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Create an OU where VMs are created. That OU must have a Citrix policy for communication with the Cloud Connectors and Citrix Cloud. See the Reference section for details.
    - Set up a group policy for the Citrix Cloud Connector™ configuration:

        a. Download the latest Group Policy Management Console provided by Citrix (CitrixGroupPolicyManagement_64.msi) from the Citrix download site.

        b. Install the MSI (that machine must have the Visual Studio 2015 runtime installed). Then create a Citrix policy that contains the Controllers policy setting. That setting specifies the Cloud Connector addresses.

- Create or use an existing NAT gateway. For more information, see NAT gateway.
- Create or use one or more existing security groups that allow the Citrix Cloud Connectors to communicate with the deployed VMs. For more information, see Control traffic to your AWS resources using security groups
- To use Windows 10 or Windows 11 desktop images with dedicated tenancy, set up BYOL for your account. You can complete this step after connecting your account. For more information, see Set up BYOL for your account.

  NOTE:

  Windows 10 N and Windows 11 N versions are not supported for BYOL.

- If you plan to use BYOL, ensure you have sufficient Windows 10 or Windows 11 licenses. For more information, see Bring Your Own Windows desktop licenses.
- Using Citrix DaaS for Amazon WorkSpaces Core automatically enables the Bring Your Own Protocol (BYOP) feature in Amazon WorkSpaces Core.

General preparation

Review each procedure before you start. Benefit: This will help the processes to be completed easily.

Create a resource location

You create a resource location in Citrix Cloud.

- A resource location contains two or more Cloud Connectors that communicate with Citrix Cloud. The servers on which you install the Cloud Connectors must be in an EC2 VPC,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

domain-joined, and have Internet connectivity. The Cloud Connectors must be in the same VPC as the directory you plan to use.

- For more information on Cloud Connectors, see Citrix Cloud Connector and how to provision them.
- The resource location can also contain your Active Directory servers. For more information, see Connect Active Directory to Citrix Cloud.

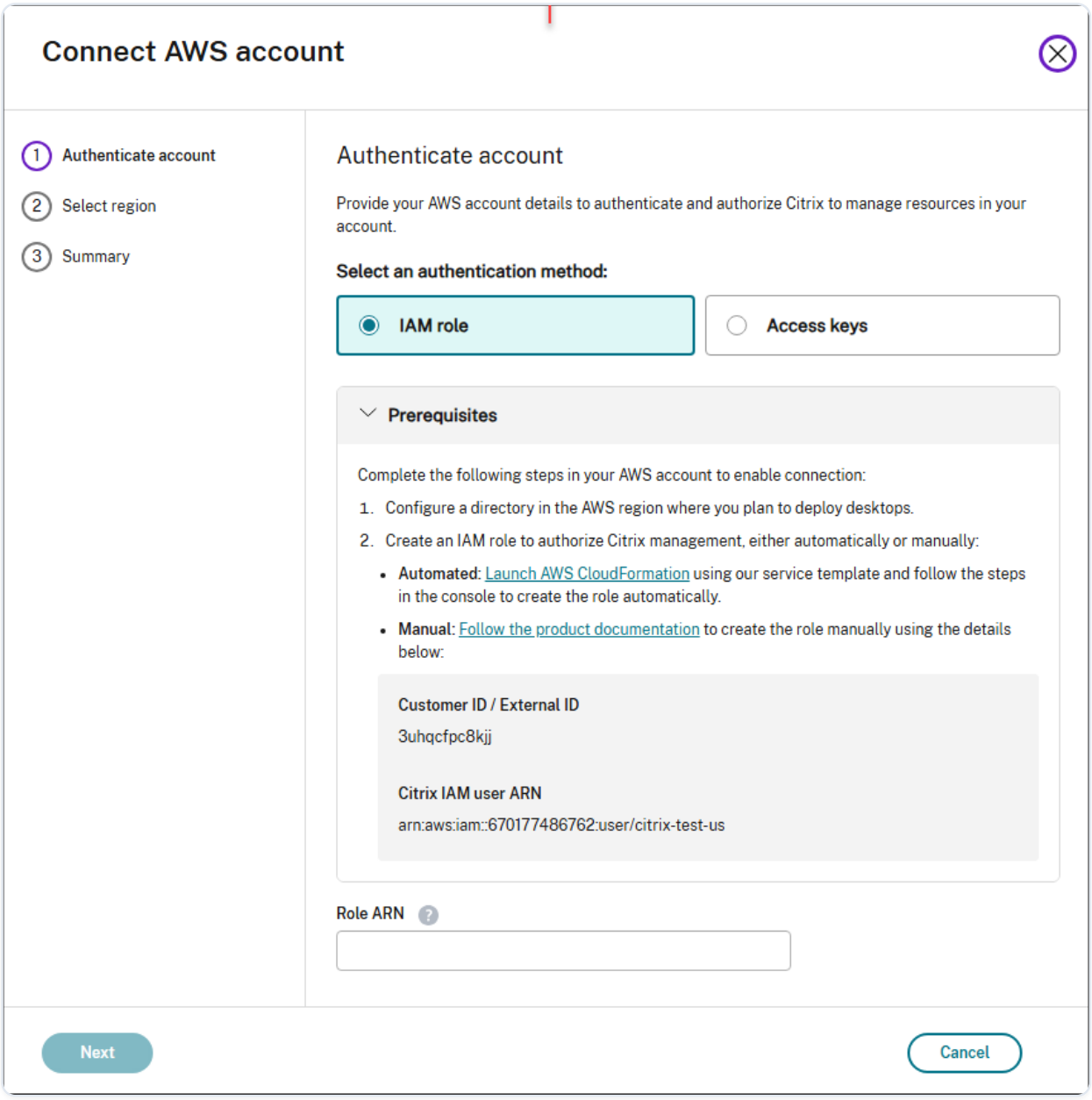
Connect your AWS account

This procedure enables permissions for the Citrix DaaS to connect to AWS.

To connect your AWS account, follow these steps:

1. In the DaaS tile, click **Manage** to open **Studio**.
2. In the left pane, select **Quick Deploy > Amazon WorkSpaces Core > Accounts**, then click **Connect account**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. In the **Authenticate account** page, complete these steps:

   a. Expand the **Prerequisites** panel to review the setup requirements.

   b. In the **Prerequisites** panel, download the AWS CloudFormation template from the **Connect account** wizard and save it locally. You will upload this template later when you create the AssumeRole stack in AWS.

   c. In the **Role ID** field, enter the Amazon Resource Name (ARN) of the role that authorizes Citrix to manage your resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP:

- The Role ID can be found in the AWS management console by navigating to **IAM > Roles**.
- If you are using the `CloudFormation` script, then navigate to CloudFormation and click the corresponding stack that was used to create the role. Navigate to the **Resources** tab and click the resource with LogicalID `CitrixAssumeRole`.

d. Enter a friendly name for the account in the **Name** field.

e. Click **Next**. The **Pick region** page opens.

NOTE:

- You cannot connect two accounts in the same region for the same AWS account.
- To create an AssumeRole, see Create AssumeRole for Amazon WorkSpaces Core integration.

4. On the **Pick region** page, select the region where you want to deploy your desktops and click **Next**. The **Summary** page opens.
5. On the **Summary** page, review the information you provided. Click **Connect**. The connection process might take several hours to complete.

NOTE:

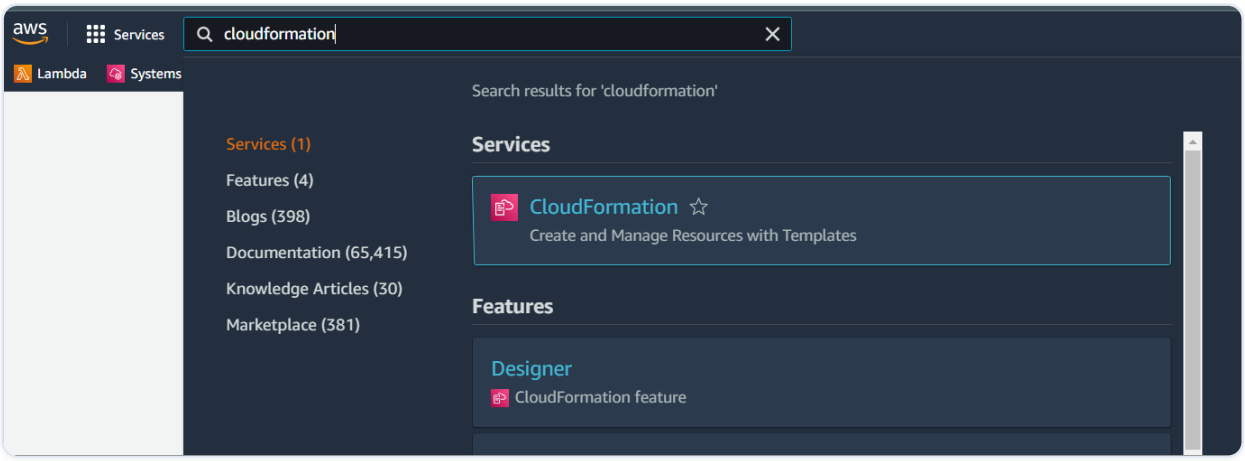
After you connect your account, you can configure BYOL at any time. For more information, see Set up BYOL for your account.

Create AssumeRole for Amazon WorkSpaces Core integration

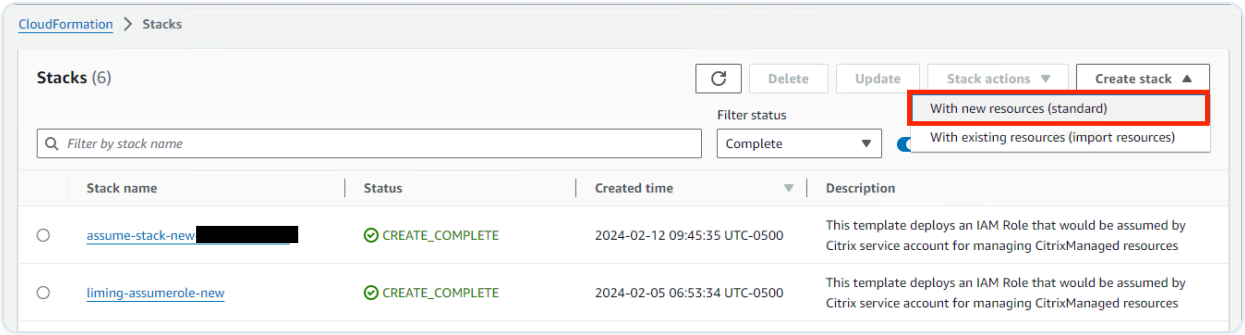
To create AssumeRole for Amazon WorkSpaces Core, follow these steps:

1. In your browser window, open the **Amazon Web Services** website and sign in.
2. In the **Search** field, type **cloudformation** and press **Enter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Under **Services** select **CloudFormation**. The **Stacks** window opens.

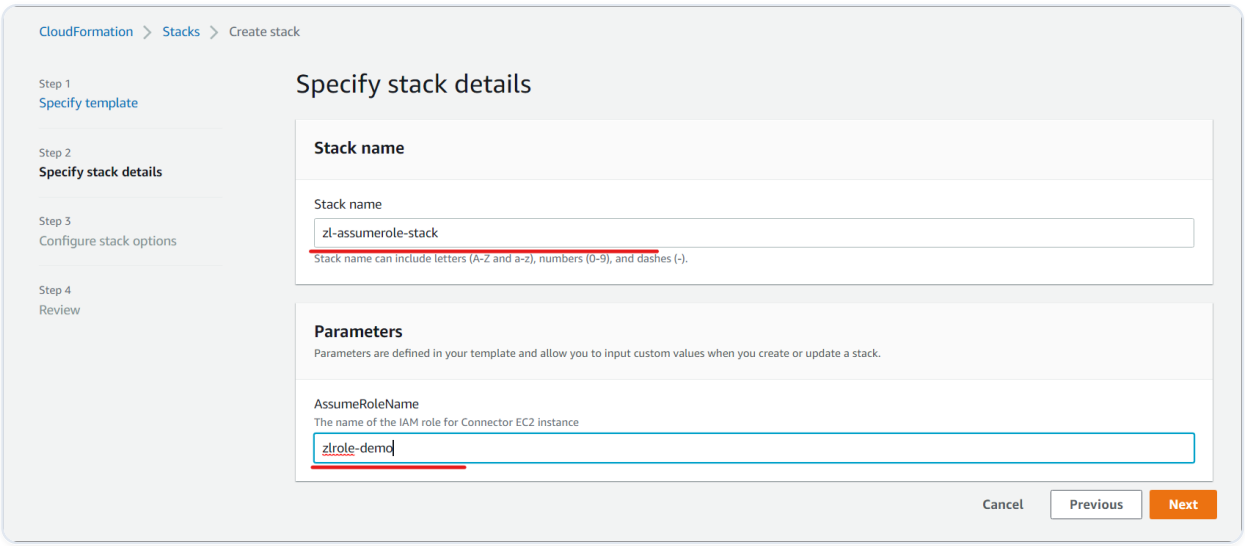


4. Click **Create stack > With new resources (standard)** at the top right corner. The **Create stack** window opens.

   a. Under **Prerequisite – Prepare template**, select **Template is ready**.

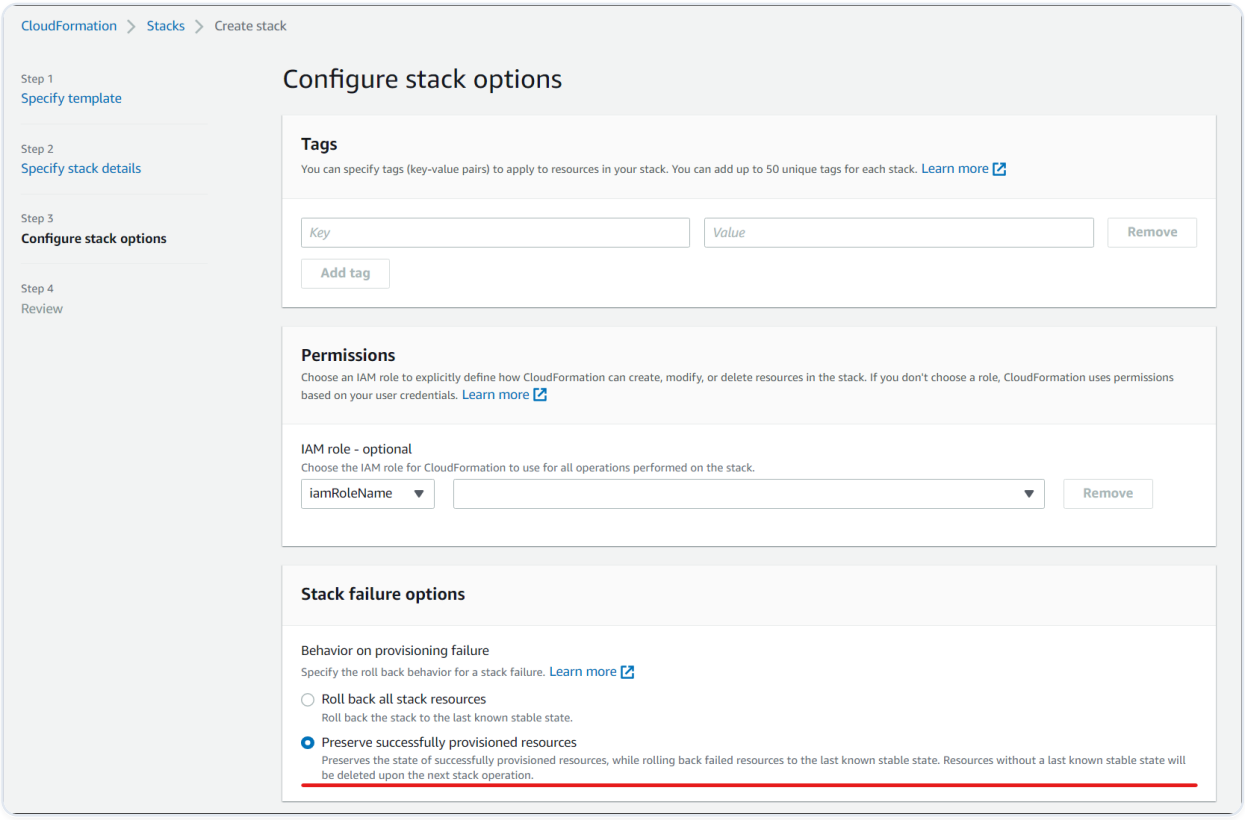
   b. Under **Specify template**, click **Upload a template file > Choose file** and click **Next**. The **Specify stack details** pane opens.

5. In the **Specify stack details** pane, provide a **Stack name** and **AssumeRoleName** and click **Next**. The **Configure stack options** pane opens.

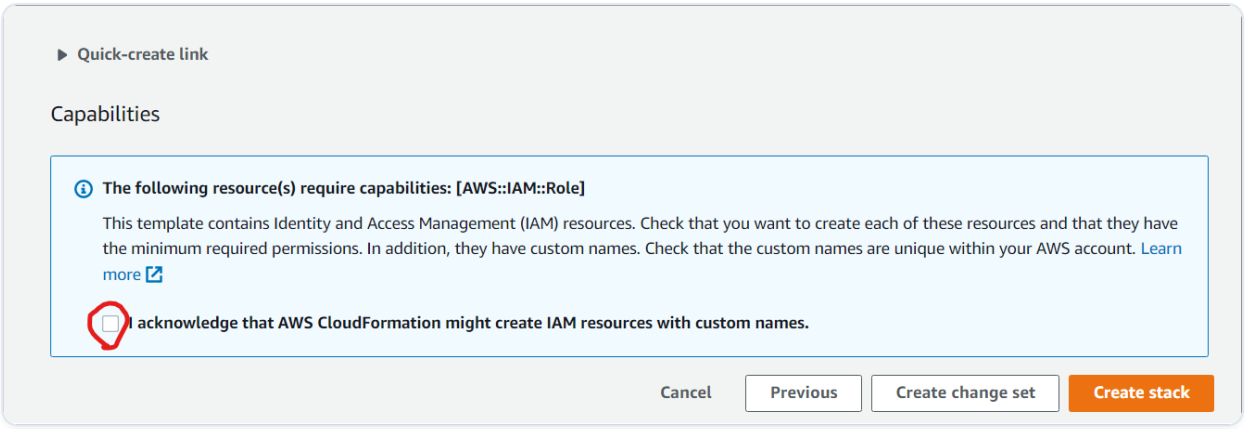


© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. In the **Configure stack options** pane, select the **Preserve successfully provisioned resources** option. This option preserves the state of successfully provisioned resources. Resources without a last known stable state are deleted upon the next stack operation.

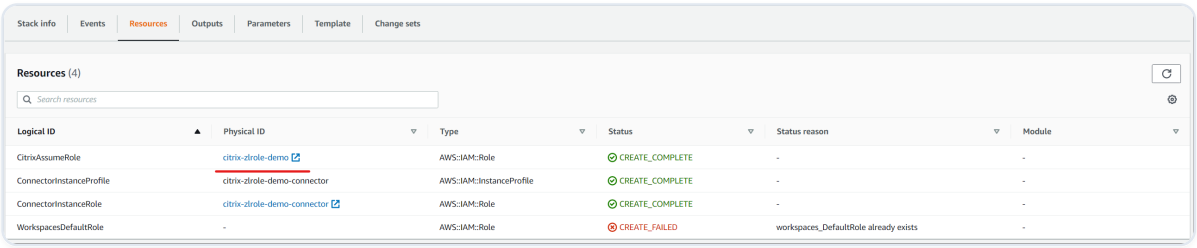


7. In the **Capabilities** pop-up window, select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox and click **Create stack**.

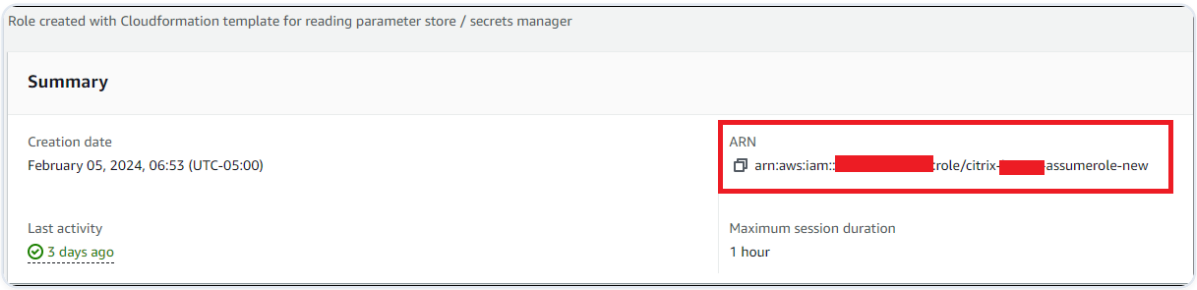


- The **Events** tab shows the status of the Stack created.
- In the **Resources** tab, select the Physical ID corresponding to the **AssumeRole** created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The Summary pane shows the **Amazon Resource Name** (ARN) generated.



NOTE:

Stack creation might fail because **workspaces_DefaultRole** has already been created. This does not affect the **AssumeRole** creation.

8. Resume the procedure from step 3 in Connect your AWS account.

(Optional) Set up BYOL for your account

Bring Your Own License (BYOL) lets you import and use Windows 10 or Windows 11 desktop images for your Citrix DaaS for Amazon WorkSpaces Core deployment. BYOL enables dedicated tenancy for directory connections and access to EC2-based machine images.

IMPORTANT:

Enabling BYOL is a permanent change for your AWS account and can only be reversed by removing all resources and contacting AWS support.

You can set up BYOL for an authenticated AWS account from the **Accounts** list or from the account detail panel.

Prerequisites:

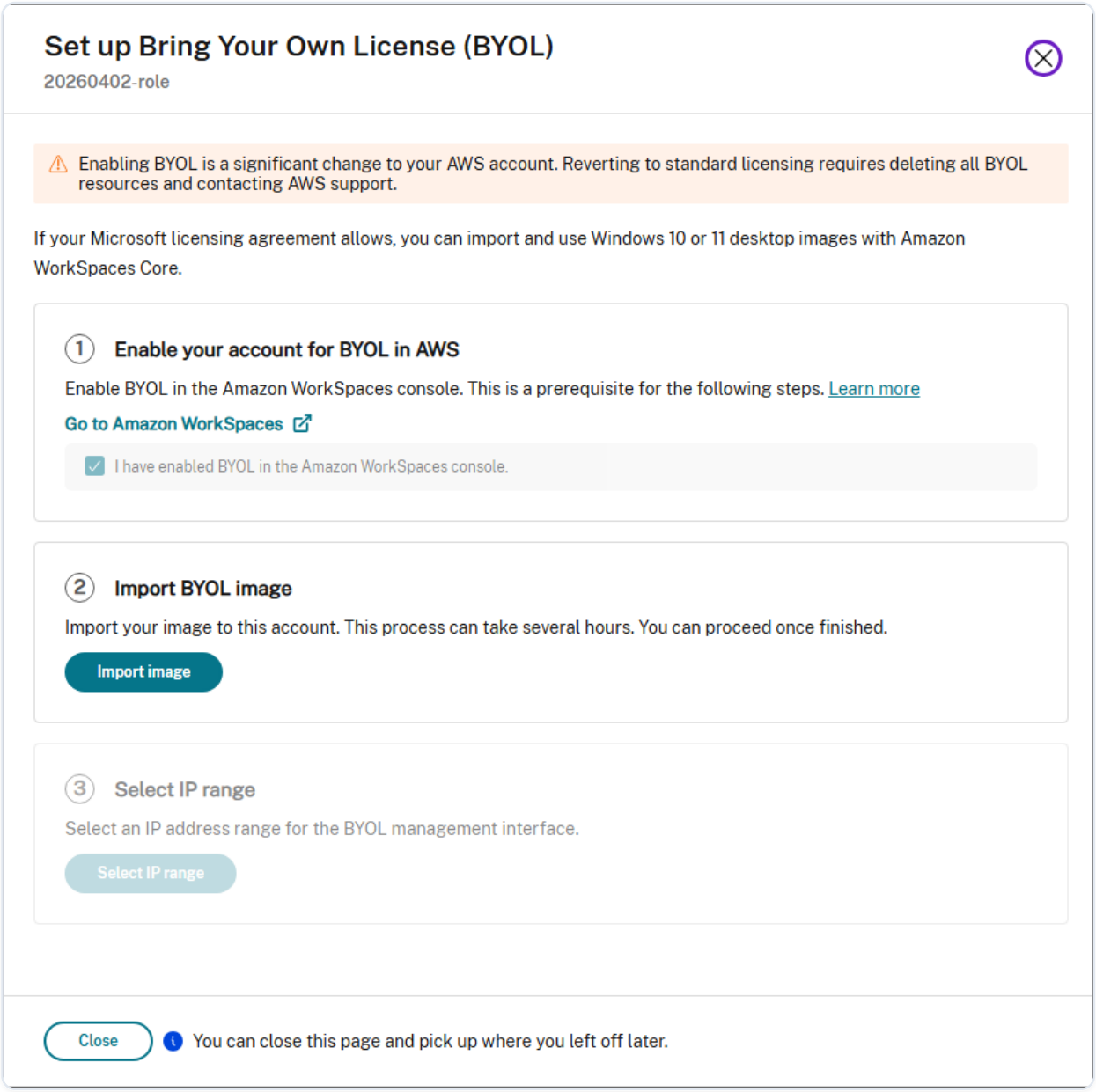
- The AWS account is in the **Authenticated** state.
- BYOL has not yet been configured for the account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- BYOL is enabled in the AWS WorkSpaces Console for your account. To enable it, contact your AWS account manager, sales representative, or the AWS Support Center. For more information, see Enable BYOL for your account using the Amazon WorkSpaces console.

To set up BYOL for your account, follow these steps:

1. In **Web Studio**, go to **Quick Deploy > Amazon WorkSpaces Core > Accounts**.
2. Select the AWS account for which you want to set up BYOL.
3. Click **Set up BYOL**. The **Set up BYOL** wizard opens.



4. On the **Enable your account for BYOL in AWS** step:
   a. Click **Go to Amazon WorkSpaces** to open the AWS WorkSpaces Console and enable BYOL for your account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. After enabling BYOL in AWS, select the **Confirm I've enabled BYOL** checkbox.

c. Click **Next**.

5. On the **Import BYOL image** step, click **Import image** to import a Windows 10 or Windows 11 desktop image into your account.

   NOTE:

   Importing an image might take several hours. You can close this page and return later to check the import status.

After BYOL setup is complete, the account detail panel shows the BYOL status, IP range, and available images.

Create a directory connection

NOTE:

Deregister your AWS Directory at the beginning of this step. After you create a Directory Connection with Citrix DaaS, the selected directory gets registered to create Amazon WorkSpaces with Citrix DaaS.

This procedure creates a connection that allows access to your organization's Active Directory.

Prerequisites:

- A resource location containing two Cloud Connectors.
- A security group.
- An OU in your Active Directory.

For prerequisite details, see Before you start.

You can start this procedure from one of two places:

- A link on the Get Started checklist.
- From Studio, select **Studio > Quick Deploy > Amazon WorkSpaces Core > Directory connections**. Then click **Create Directory Connection**.

Follow the **Create directory connection** sequence:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Connect directory:** Select the account from the drop-down menu. Select either **Dedicated** or **Shared** for the tenancy.
2. **Resource location:** Select the account and directory. (The selected account must have at least one directory.)
    - Select two subnets in which the desktop machines will be deployed. The subnets must be in appropriate availability zones.
    - Specify a friendly name for this connection.
    - When you're done, click **Next**.
3. **Virtual machine settings:** The settings you select apply to all VMs that use this directory connection.
    - The OU selected must match the OU targeted by the Citrix Group Policy.
    - Select a security group.
    - Indicate whether you want to give administrator privileges to each user assigned to VMs.

Import an image

This procedure enables you to create a desktop experience for your users. You can now import two types of images:

- EC2 Image - To import this image, the prerequisite is to install Citrix Virtual Delivery Agent and all its drivers. The image must also be prepared for BYOL. A BYOL script is available at: BYOLChecker.zip.
- Workspace Image - To import this image, the prerequisite is to install Citrix Virtual Delivery Agent and all its drivers.

To import the image, follow the steps:

1. In **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, click **Images**.
2. In **My Images**, click **Import Image**.
    a. **Prerequisites:** Provides the prerequisites details for EC2 image and Workspace image. Click **Next: Choose image**.
    b. **Choose image**
        - Provide a friendly name for the image.
        - Select an account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- From the **Image** drop-down list, you can select EC2 or WSI type of images.
  - If you select **EC2**, then choose the application to install from the **Application** drop-down menu and click **Next: Summary**. EC2 type images support only single-sessions.
  - If you select **WSI**, then ensure that the session support and ingestion process align with the image setup. Although a mismatch does not overwrite the image's settings, but might cause deployment failure due to incompatibility. Select session support as single or multi-session.
- Provide a description and click **Next: Summary**.
- Click **Next**. The **Summary** page opens.

3. In the **Summary** page review the information you provided and click **Import Image**.

> **NOTE:**
>
> Importing an image might take several hours.

4. Select any image and click **View Detail**. The details page shows the options selected while creating the images, such as Account, Session support, Tenancy, Applications, and others.

> **NOTE:**
>
> When you create a deployment, in the **Image and performance** page:

- If the **Directory connection** selected has a dedicated tenancy, then the images listed are only single-sessions. In the **Desktops** page you can choose to create desktops with or without assigning users.
- If the Directory connection selected has a shared tenancy, then the images listed are both single and multi-sessions. If you select an image with multi session, then in the **Desktops** page, only **Create desktops without assigning users** option is enabled.

Requirements for Dedicated Tenancy Images

- The images must be either Windows 10 Pro or Windows 11 Pro.
- Run the BYOLChecker script during the image preparation.
- The image can only be set in single-session support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When creating an AMI image in EC2, the snapshot must be unencrypted.
- The default ingestion protocol during image import is regular. However, customers can opt for the graphical G4DN ingestion protocol, which installs additional drivers and requires higher-tier machines.
- During image import, customers can add an office application to be installed. This will limit workspace creation to preassigned users deployment.
- The images require the directory connection to be set as dedicated.
- You can create preassigned single-session deployments or decoupled (pooled) single-session deployments.

Requirements for Default or Shared Tenancy Images

- Select the Windows Server BYOP bundle to create a workspace.
- The workspace must be unencrypted, and only the **Always On** mode is supported.
- Connect to the workspace from the connector using the private IP address via RDP and log in with the same user credentials the workspace is assigned to. The image cannot be saved if there are multiple user profiles on the machine.
- Install VDA and run the image checker application.
- VDA can be configured as either single-session or multi-session.
- Restart the workspace and save it as an image.
- After the image is saved, it can be imported into the Citrix environment.
- The default ingestion protocol during image import is regular. However, if the base bundle was G4DN-based, you can opt for the graphical G4DN ingestion protocol.
- The images require the directory connection to be set as shared.
- If you set up and saved the image as a single-session, you can create preassigned single-session deployments or decoupled (pooled) single-session deployments.
- If you set up and saved the image as a multi-session, you can only create decoupled (pooled) multi-session deployments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS, Directory Type, and Session Support Compatibility

IMAGE	SESSION SUPPORT	AWS DIRECTORY TENANCY	DEPLOYMENT TYPE	PERSISTENCE
Windows Desktop 11 Pro	Single-Session	Dedicated	Dedicated or Pooled	Persistent
Windows Desktop 10 Pro	Single-Session	Dedicated	Dedicated or Pooled	Persistent
Windows Server 2022	Multi-Session	Shared	Pooled	Persistent
Windows Server 2022	Single-Session	Shared	Dedicated or Pooled	Persistent
Windows Server 2019	Multi-Session	Shared	Pooled	Persistent
Windows Server 2019	Single-Session	Shared	Dedicated or Pooled	Persistent

NOTE:

All instances are persistent and using the pools feature, the instances are assigned on the first use basis. The instances remain provisioned without an assigned user. When a user logs in for the first time, that instance is assigned to the user for all future logins.

Integrate Microsoft Office 2019 Image when importing an image

To integrate Microsoft Office 2019 image while importing an image:

1. In **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, click **Images**.
2. In **My Images**, click **Import Image**.
3. In **Import Image > Prerequisites**, click **Next: Choose Image**.
4. In **Import Image > Choose image:**
    - Select an account from the **Account** dropdown.
    - Select an AMI from the **AMI** dropdown.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Enter the name of the image in the **Name** field.
- Select the **Include Microsoft Office 2019 Professional Plus** in the image.
- Enter a description in the **Description** field.

5. In **Import Image > Choose image**, click **Next: Summary**.
6. In **Choose Image > Summary**, ensure that **Selected** appears for **Microsoft Office 2019**.
7. In **My Images**, click **Import Image**. The status of the recently deployed image displays **importing** until the import operation completes.
8. In **My Images**, select the recently deployed image and click **View Detail**.
9. In the **Detail** panel, the **Microsoft Office 2019** field displays **Included**.

NOTE:

Only the following versions of the OS are compatible:

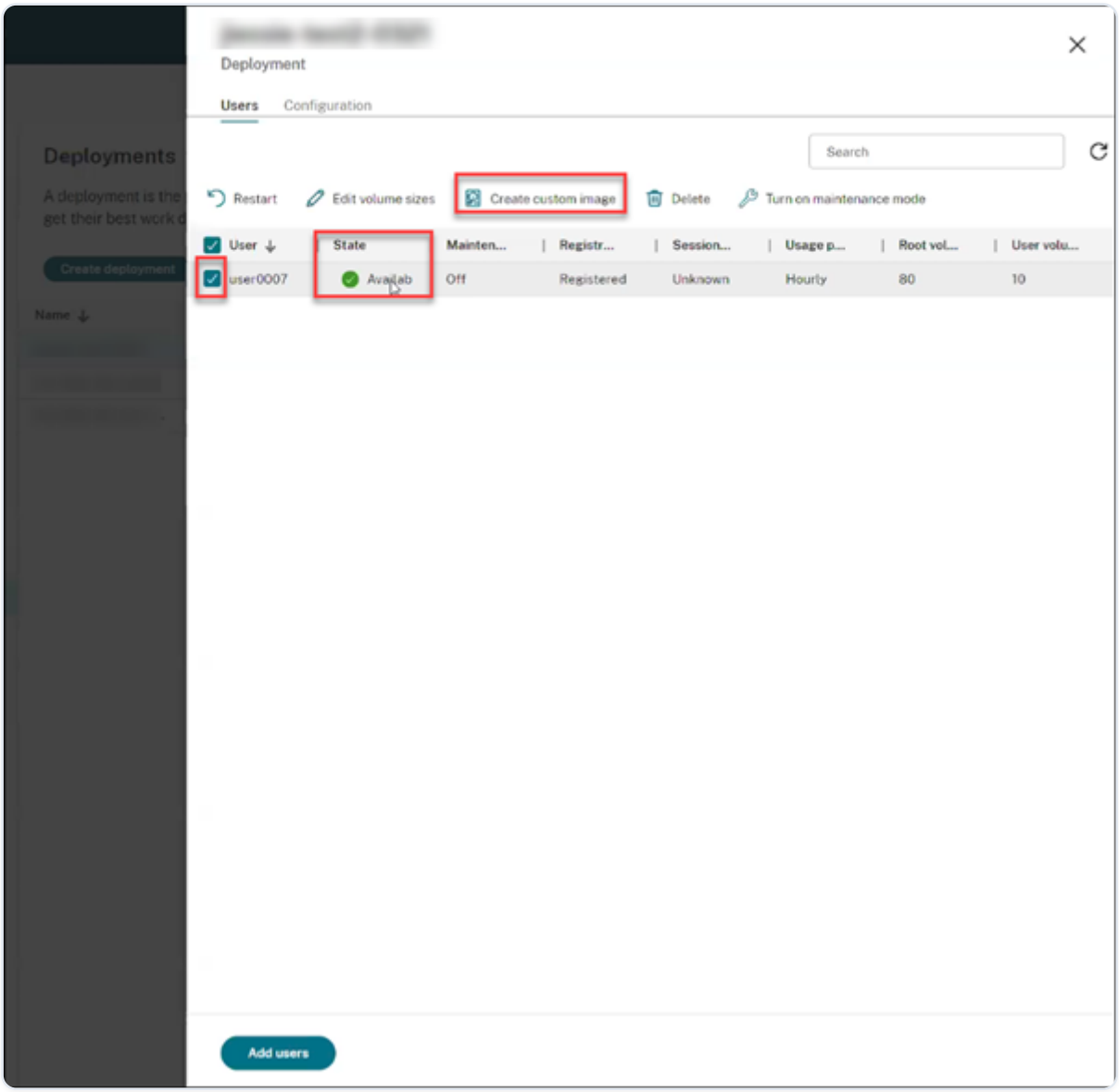
- Windows 10 Version 21H2 (December 2021 Update)
- Windows 10 Version 22H2 (November 2022 Update)
- Windows 10 Enterprise LTSC 2019 (1809) (1809)
- Windows 10 Enterprise LTSC 2021 (21H2) (21H2)
- Windows 11 Version 22H2 (October 2022 release)

Create a custom image from an existing WorkSpaces instance

To create a custom image for a user:

1. In **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, select **Deployments**.
2. Select the deployment containing machines you want to manage and click **View detail**.
3. In the **Deployment** pane, under the **Users** tab, select the **User** whose workspace state is available and click **Create custom image**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



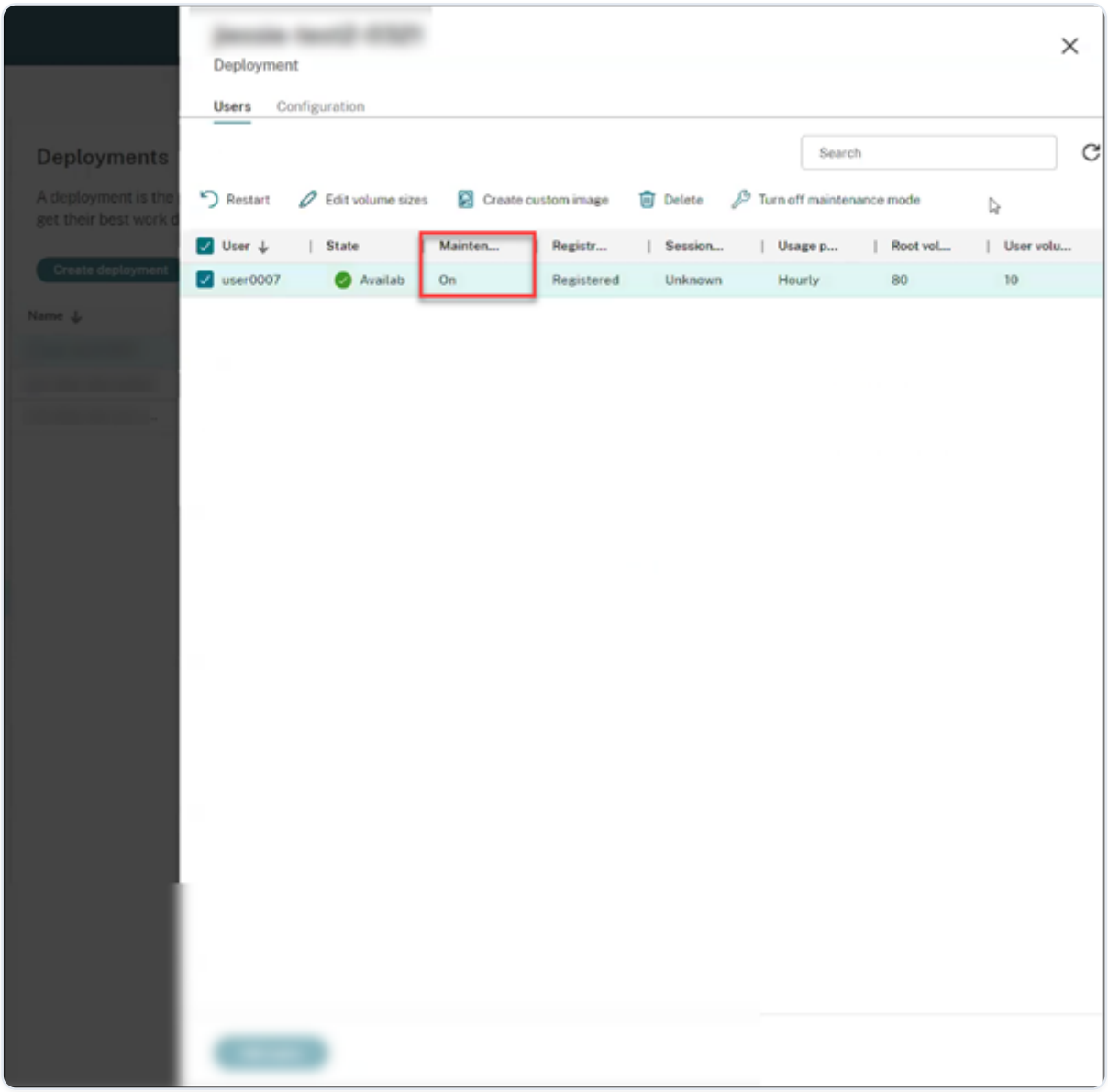
NOTE:

You can create a custom image only for the deployment whose workspace state is available.

4. In the **Create custom image** pane:
   - Verify the **Image properties**, **OS** and **Account** information of the selected user.
   - Note the warning message that indicates the time the desktop deployment will be in maintenance mode during the process.
   - Fill the mandatory fields like **Image name** and **Description**. The **Image name** field suggests the allowed characters for image names.
5. Click **Create**. The **Images** node window opens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Click the **Refresh** button. The newly created custom image is listed with the **Status** as **Pending**.
7. Select the custom image and click **View Detail**. The Image window opens with details like **Status**, **Account**, **ID**, **OS**, and **Description**.
8. Click **Deployments** in the left navigation. The **Status** of the new deployment shows as **Updating**.
9. Select the new deployment and click **View detail**.
    - In the **Deployment** pane, the **Maintenance** tab shows as **On**.



As a best practice:

- Use a separate Virtual Private Cloud (VPC) that is not connected to your production environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For Windows WorkSpaces, avoid configuring any Group Policy Objects (GPOs) before creating the image. For more information, see Best practices.
- Use a dedicated AD Connector for image creation.
- Use a dedicated OU in the Active Directory for image creation. For more information, see Best practices for successful BYOL image creation for Amazon WorkSpaces.

Create a deployment

A deployment is a group of desktops that users can access from their store. This procedure specifies the characteristics of the virtual machines to be deployed as desktops, and which AD users can use them.

NOTE:

The computer name is set by Amazon when the workspace is created and is used as an identifier to ensure accurate workspace data. You cannot modify the computer name using Citrix DaaS for Amazon Workspaces Core.

Prerequisites

Complete all the steps listed in Prepare and create a deployment.

1. In **Web Studio > Quick Deploy > Amazon WorkSpaces Core > Deployments**, click **Create deployment**.
2. In the **Image and performance** page,
    a. if you select a dedicated tenancy, as the Directory connection, then the image drop down lists the images that have Dedicated tenancy. Images with Dedicated tenancy support only single-sessions.
    b. if you select a shared tenancy as the Directory connection, then the Image drop down lists the images that have Default tenancy. Images with Shared tenancy support both single and multi-sessions.
    c. Select the **Performance** and **Root volume sizes**. Click **Next: Encryption**.
3. **Encryption**: In the **Select encryption key preference** section:
    a. The **Use AWS managed KMS key** option is selected by default. This encrypts both root and user volume and is managed by AWS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. If you select the **Use customer managed key** option, ensure to first create the key in **AWS Key Management**. Once created, enter the key into the **Key Alias** field and click **Next: Desktops**.

> **NOTE:**
>
> Encryption keys can be found in the **Key Management Service (KMS)** console under **AWS managed keys** or **Customer managed keys**.

4. **Desktops**:

   a. A new option to select **Create desktops without assigning users**, is added. If you select this option, it is recommended to configure the user profile location to be stored on the D: drive or at an external location. By default, the user profile is stored on the C: drive. The user data and settings on the C: drive are lost if you rebuild the WorkSpace. Specify the number of desktops you want to add to the deployment. The **Desktop assignment type** for this option is **Random pool unassigned**. Click **Next: Summary**.

> **NOTE:**
>
> The **Create desktops without assigning users** option is not available for images with AWS provided applications. Therefore, you must assign users while creating desktops.

   a. If you select the existing **Assign users while creating desktops** option, search and select the users who will be allowed to access the desktops. If you want to customize the volume sizes for a user, select **Edit user and root volume sizes**, and then specify the sizes. The **Desktop assignment type** for this option is **Static preassigned**. Click **Next: Summary**.

5. **Summary:** Review the information you provided and provide a **Deployment name**. Click **Create deployment**. The **Deployment** page shows the new **Desktops** column with the assigned desktop details.
6. Re-sync: Click Re-sync for a deployment that is in Pending state or if the number of machines listed in a deployment does not match with the number of machines listed in AWS.
7. Select a deployment and click **View detail**. The deployment details page shows three tabs:

   a. **Desktops**: Select a desktop and the settings to modify is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **Applications**: This tab allows you to add new applications and to delete the existing applications. For more information about adding applications to an existing deployment, see Step 6. Applications.

c. **Users**: This tab is available only for unassigned deployments to assign users or groups to launch the desktop. Click **Add**. Update the required settings and click **Find now**. You can select more than one user from the table and click **Ok > Done**. You can add more users and also delete an existing user by selecting appropriate options.

d. **Configuration**: This tab shows the assignment type of the selected desktop. If it is an unassigned desktop, then the **Desktop assignment type** is **Random pool unassigned**.

Integrate Microsoft 365 Windows apps

To integrate Microsoft 365 Apps, see Microsoft 365 Apps for enterprise now available on Amazon WorkSpaces services and Microsoft 365 Bring Your Own License (BYOL).

Manage machines in a deployment

In addition to the machine management features described in Manage machine catalogs, for some actions, you can select machines to manage from a deployment.

To manage machines in a deployment:

1. In **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, select **Deployments**.
2. In the **Deployments** pane, select the deployment containing machines you want to manage.
3. Click **View details**.
4. In the **Deployment details** pane, select the machine you want to manage.
5. From the actions displayed, select the action you want to perform on the machine:

- Click **Edit volume size** to change the volume size of the machine.
- Click **Delete** to delete the machine from the deployment and AWS. If a machine is in a delivery group, it can be deleted only if it is maintenance mode.
- Click **Turn maintenance mode on/off** to turn maintenance mode on (if it is off) or off (if it is on) for the machine.

Add applications to a deployment

To add applications to an existing deployment:

1. In **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, select Deployments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. In the Deployments pane, select the deployment to which you want to add the applications.
3. Click Add applications. The Add Application pane opens.
4. Click the Add menu and select one of the following sources to add the applications:
    - From Start menu
    - Manually
    - Application packages
    - Existing
    - Application group

For more information about adding applications to an existing deployment, see Step 6. Applications.

Use persistent desktops with a non-persistent user profile

Workspace Environment Management™ can be used to configure Profile Management settings to enable persistent desktops with non-persistent user profiles. This provides you with a customizable desktop experience while maintaining easy management and centralized storage of user profiles, creating a flexible and scalable solution for virtual desktop environments. Do the following to configure the setting:

1. From the WEM console, navigate to **Configuration Set > Policies and Profiles > Citrix Profile Management Settings**.
2. Select **Enable Profile Management Configuration** and navigate to **Profile Handling** tab.
3. Select **Delete locally cached profiles on logoff**.

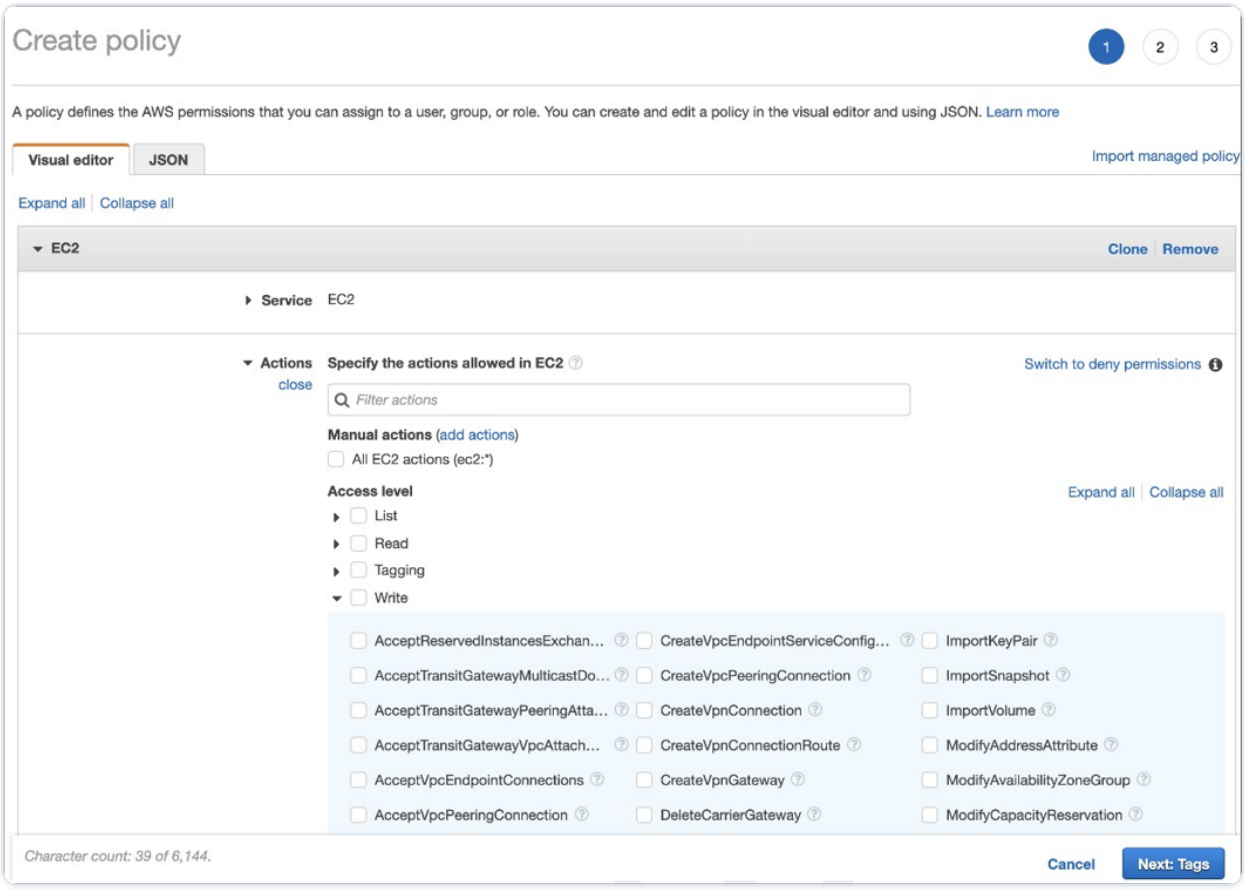
Reference

AWS account programmatic access permissions

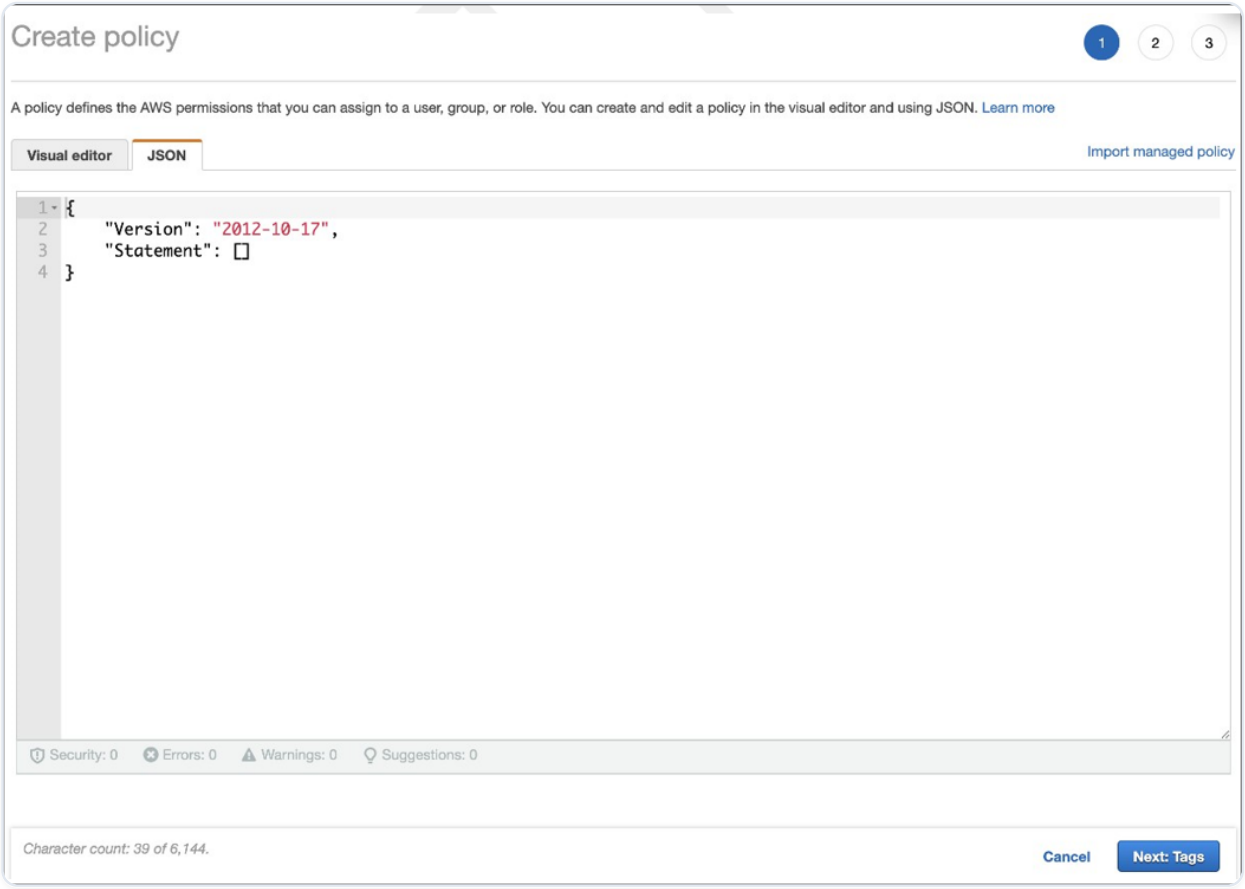
The AWS user account must have certain programmatic access permissions to make API calls to the AWS resource layer. Programmatic access creates an access key ID and a secret access key. You can create a policy containing these permissions in the IAM console. As shown in the following graphics, you can use the visual editor (adding the permissions one by one) or the JSON (adding the snippet below). For more information, see Creating an IAM user in your AWS account.

- On the **Visual editor** tab, add the permissions one-by-one.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- On the **JSON** tab, add the snippet shown after the following graphic.



Required permissions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                    "workdocs:DeregisterDirectory",
                    "workdocs:RegisterDirectory",
                    "workdocs:AddUserToGroup",
                    "ec2:ImportInstance",
                    "ec2:DescribeImages",
                    "ec2:DescribeImageAttribute"
                    "ec2:CreateKeyPair",
                    "ec2:DescribeKeyPairs",
                    "ec2:ModifyImageAttribute",
                    "ec2:DescribeVpcs",
                    "ec2:DescribeSubnets",
                    "ec2:RunInstances",
                    "ec2:DescribeSecurityGroups",
                    "ec2:CreateTags",
                    "ec2:DescribeRouteTables",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    "ec2:DescribeInternetGateways",
                    "ec2:CreateSecurityGroup",
                    "ec2:DescribeInstanceTypes",
                    "servicequotas:ListServices",
                    "servicequotas:GetRequestedServiceQuotaChange",
                    "servicequotas:ListTagsForResource",
                    "servicequotas:GetServiceQuota",
                    "servicequotas:GetAssociationForServiceQuotaTemplate",
                    "servicequotas:ListAWSDefaultServiceQuotas",
                    "servicequotas:ListServiceQuotas",
                    "servicequotas:GetAWSDefaultServiceQuota",

"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",

"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",

"servicequotas:ListRequestedServiceQuotaChangeHistory",

"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
                    "sts:DecodeAuthorizationMessage",
                    "ds:*",
                    "workspaces:*",
                    "iam:GetRole",
                    "iam:GetContextKeysForPrincipalPolicy",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    "iam:SimulatePrincipalPolicy"



                ],

                "Resource": "*"

            }

        ]

}
```

Citrix DaaS™ for Google Cloud

With Studio, you can deploy and manage virtual apps and desktops on Google Cloud. For information about supported features, see the Citrix Virtual Apps and Desktops feature matrix.

To deploy and manage Google Cloud apps and desktops using Studio, follow these steps:

1. Order Citrix DaaS for Google Cloud from the Google Cloud Marketplace.
2. Sign in to Citrix Cloud.
3. In the **DaaS** tile, click **Manage** to open Studio.
4. Deploy virtual apps and desktops using one of these workflows provided in the **Manage** section:

    - Quick Deploy (recommended for fast, guided deployment). For more information, see Quick Deploy for Google Cloud.

      NOTE:

      To perform advanced configurations or management options, convert your deployment to the full configuration mode. For more information, see Convert a deployment.

    - Full Configuration (recommended for advanced configuration requirements). For more information, see Get started: Plan and build a deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For step-by-step instructions on deploying and configuring virtual apps and desktops on Google Cloud, see this Citrix Tech Zone article: Citrix virtualization on Google Cloud. This article covers defining the deployment architecture, preparing the Google Cloud project, configuring network services, and deploying Active Directory.

Quick Deploy for Google Cloud

Quick Deploy for Google Cloud provides a simplified user experience for connecting Citrix DaaS to Google Cloud and creating a deployment of virtual apps and desktops. Its streamlined user interface guides admins along the key steps of this journey and removes unnecessary complications.

This interface offers basic configuration, without advanced features.

To deploy virtual apps and desktops using Quick Deploy, follow the onscreen wizard to complete these steps:

1. Launch Quick Deploy for Google Cloud
2. Create a resource location
3. Add a Google Cloud project
4. Create a network connection
5. Create a deployment

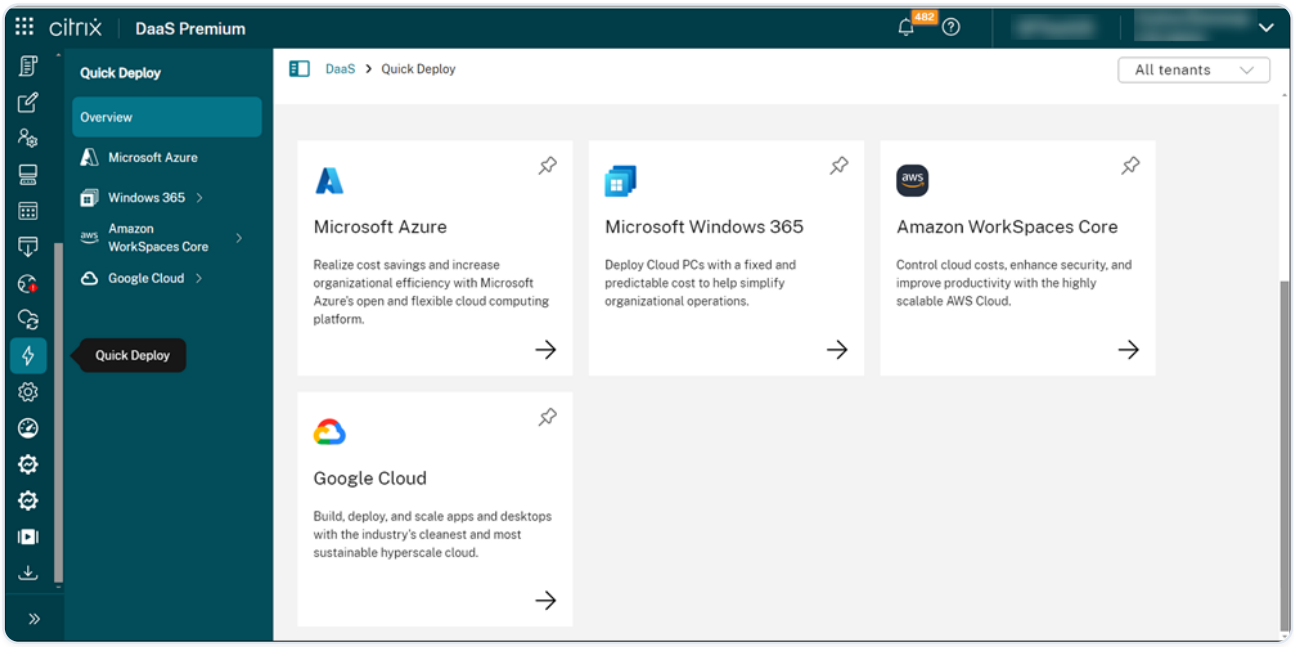
After you create a deployment, perform these tasks as necessary:

- Grant users access rights
- Convert a deployment to the full configuration mode for advanced settings and management option.

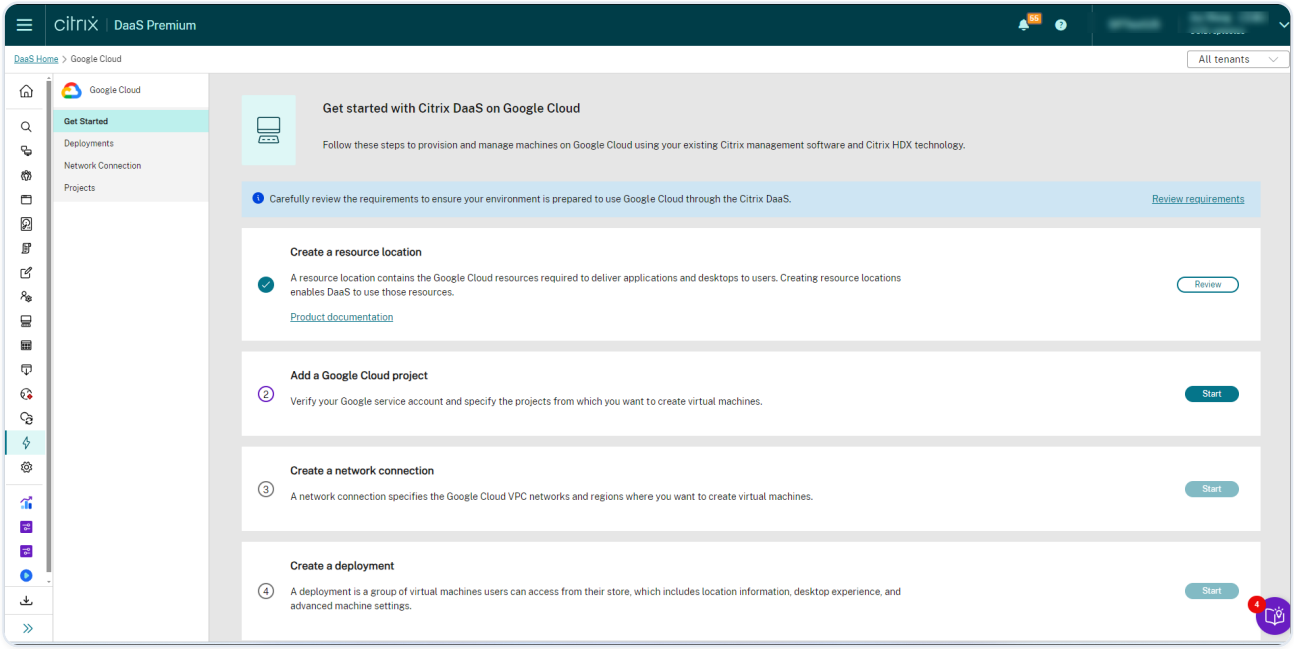
Launch Quick Deploy for Google Cloud

Quick Deploy for Google Cloud can be accessed from within Studio, by selecting the Quick Deploy node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



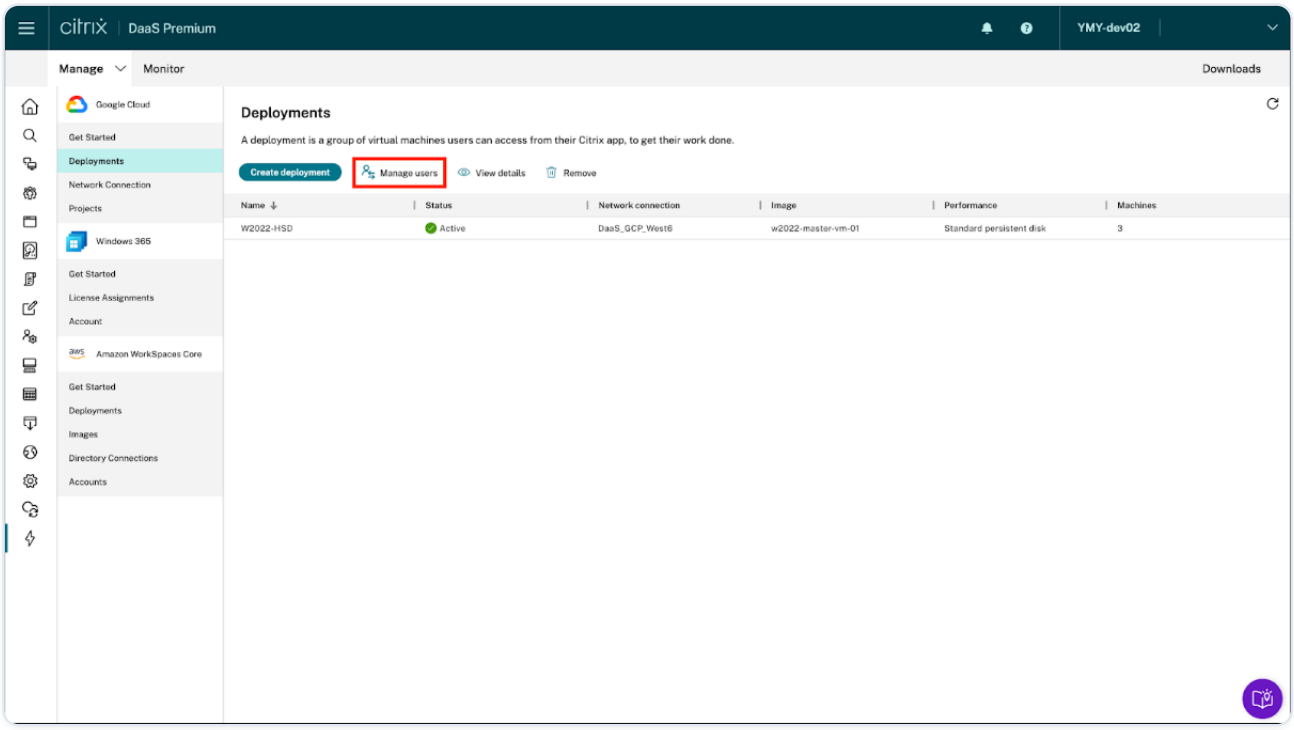
To begin the Quick Deploy process, review the steps provided on the Get Started page. Start with **Review requirements**.



Manage user access rights

After a deployment is created, grant users access permissions as necessary. To complete this task, select the respective deployment and then select **Manage users**.

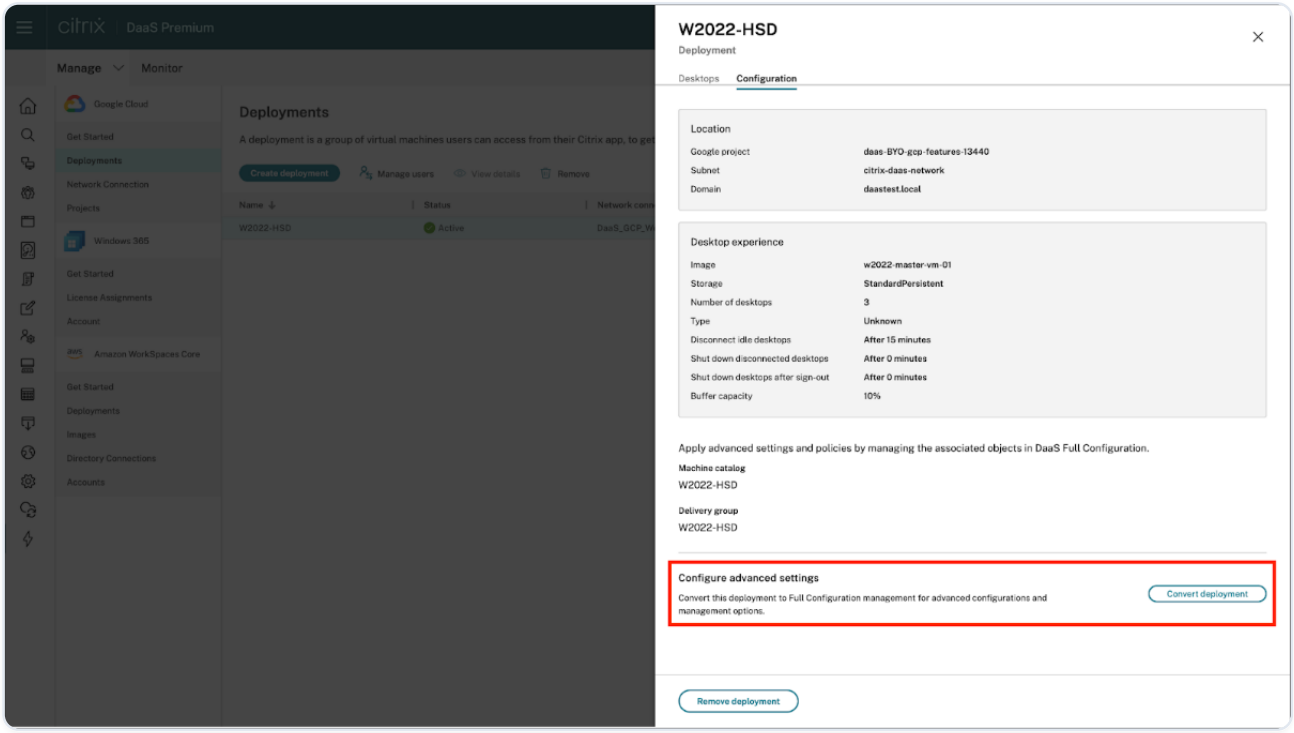
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Convert a deployment

Before you perform any advanced configurations or management activities, ensure you convert the deployments. To convert a deployment:

1. Click **Deployments** in the left navigation.
2. Select a deployment and click **View details**.
3. Click the **Configuration** tab and select **Convert deployment**.



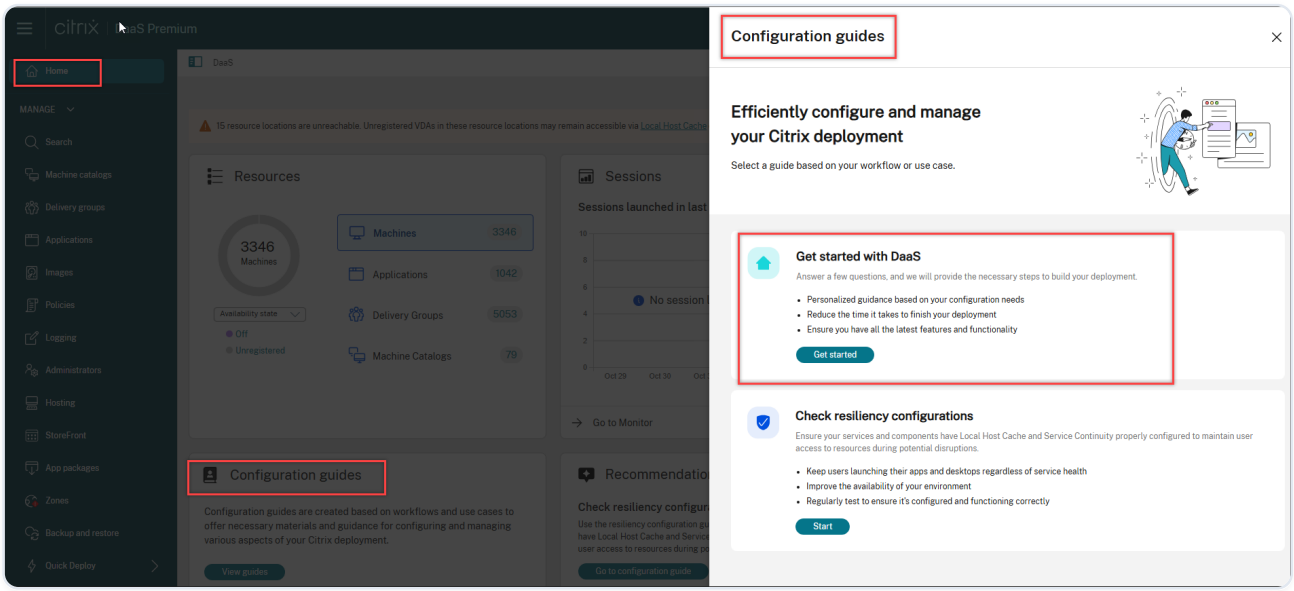
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Once a deployment is converted, the action is irreversible and the converted deployments no longer appears in Quick Deploy.

Use DaaS get-started guide

DaaS get-started guide streamlines and simplifies the DaaS deployment process for both new and experienced administrators. Using the guide, you can quickly set up your DaaS deployments by answering a series of questions.



This article walks you through the processes of setting up five typical DaaS deployment scenarios.

Benefits

Benefits of using this guide include:

- **Easy to get started**. This guide connects essential deployment steps through a questionnaire-led, step-by-step workflow. If you're a new administrator, you can quickly set up your deployment while learning concepts and terminology through contextual help.
- **Simplify complex configurations**. This guide provides pre-configured settings wherever necessary and provides access to Studio for advanced configurations. If you're an experienced administrator, you can use the guide as a starting point for complex configurations.

Supported deployment scenarios

This guide provides quick deployments for these scenarios:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHAT TO DELIVER?	MACHINES ALREADY EXIST?	MACHINE TYPE	REMARK
Virtual apps and desktops	No	Virtual machines (Provisioned by DaaS)	Power managed
Virtual apps and desktops	Yes	Virtual machines or blade PCs	Power managed
Virtual apps and desktops	Yes	Physical or virtual machines	Not power managed
Office PCs	Yes	Physical machines	Power managed
Office PCs	Yes	Physical machines	Not power managed

See the following sections for detailed instructions:

- Deliver apps and desktops from scratch (power managed)
- Deliver apps and desktops using existing machines (power managed)
- Deliver apps and desktops using existing machines (not power-managed)
- Deliver office PCs (power managed)
- Deliver office PCs (not power-managed)

Terminology

The following are DaaS-specific terms:

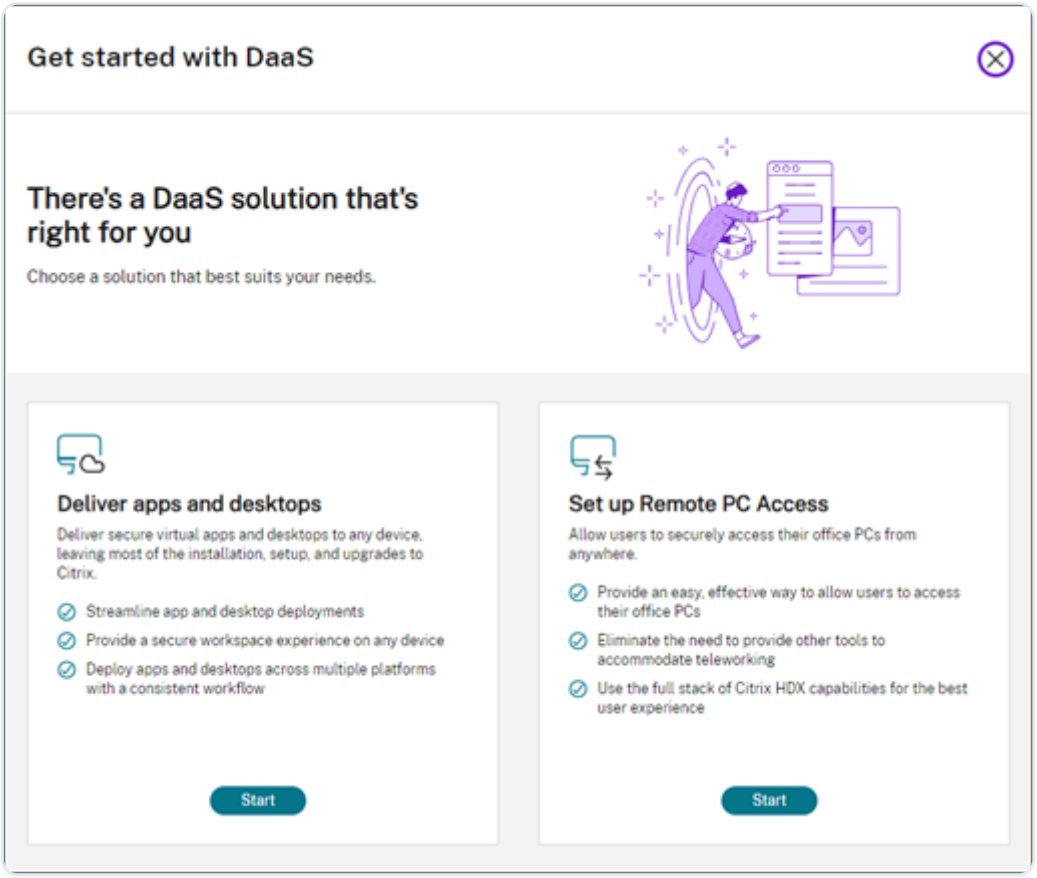
- **Resource location.** Contains the resources required to deliver apps and desktops to users.
- **Host connection.** Connects DaaS to a host (hypervisor or cloud service) in a resource location. Creating host connections is required when you want to create and manage machines on hosts or to power manage existing machines.
- **Master image.** Serves as a template for replicating virtual machines on your host. It includes the operating system, applications, Virtual Delivery Agent (VDA), and other software.
- **Machine catalog.** Collection of identical machines. They can be virtual or physical depending on your needs. You can create a machine catalog to create identically configured machines on a host or import machines into DaaS for management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Delivery group.** Contains machines from machine catalogs. Also, it specifies which users can use those machines and which applications and desktops are available to those users.
- **Machine Profile.** Specifies the properties of virtual machines. VMs in a catalog can inherit properties from a machine profile.

Access the guide

1. Go to the **DaaS > Home** page.
2. Locate **Get started with DaaS**.
3. Click **Get Started** to initiate your deployment process.



NOTE:

You can exit the process at any time by clicking **Close** and the guide saves your settings automatically. To continue your configuration, click **Continue**. To start fresh, click **Start over**.

Deliver apps and desktops from scratch (power managed)

This section guides you through the deployment process of creating VMs and delivering apps and desktops using them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

Before you start, you need:

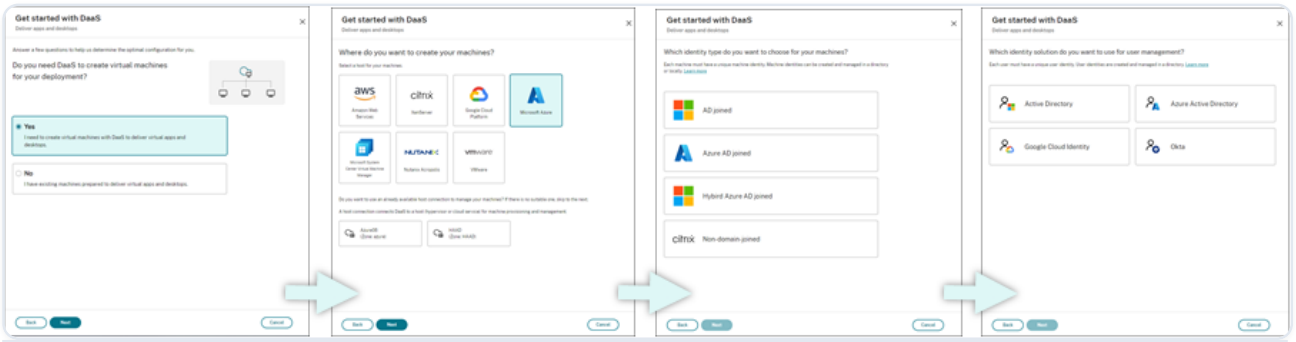
- Connectivity from Citrix Cloud™ to the target identity provider

  For more information, see the corresponding section in Identity providers.
- Role: Full Administrator or Cloud Administrator
- Required permissions on the target hypervisor or cloud service.

  For more information, see the corresponding sections in the Create and manage connections.
- Administrator credentials for VM account creation

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings. See the following table for details.



#	SETTING	DESCRIPTION
1	Specify whether VM creation is needed	Select **Yes**.
2	Select the host type	Select a host type for your deployment.
		Options: AWS, XenServer (formerly Citrix Hypervisor™), Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis, and VMware

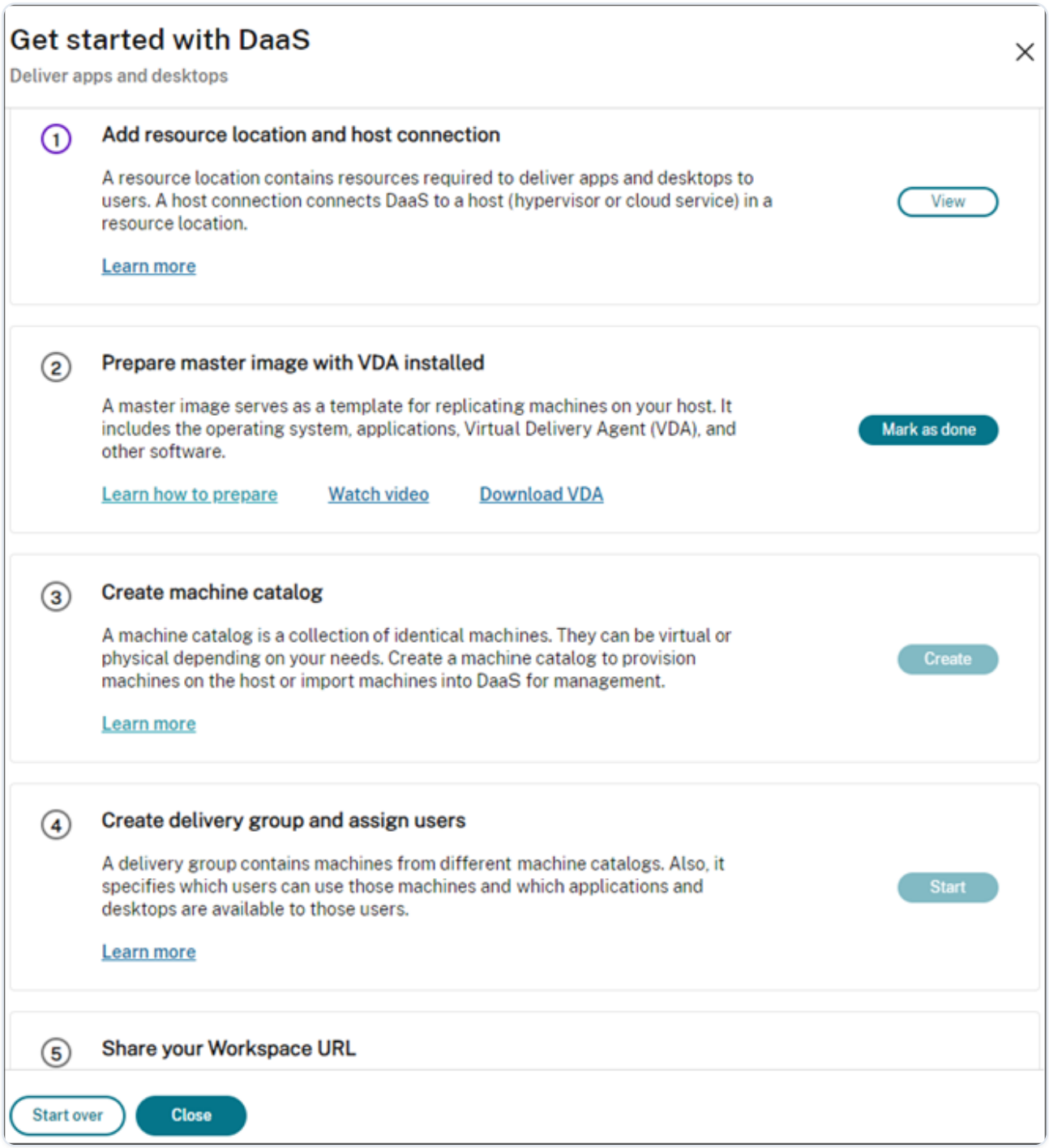
© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING	DESCRIPTION
3	Select the machine identity type	Select an identity type for machine management.
		Options: AD joined, Microsoft Entra joined, Microsoft Entra hybrid joined, and Non-domain-joined
4	Select the user identity type	Select an identity type for user management.
		Options: Active Directory, Microsoft Entra ID, Google Cloud Identity, and Okta

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear as follows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location and host connections

Set up your resource location by installing Cloud Connectors and configure connections to hypervisors or cloud services in the location.

1. Name the resource location.
2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Add and configure host connections for the resource location. Detailed settings of a connection include:

   - Connection details, such as the connection address, user name, and password.
   - Storage resources
   - Network resources

   NOTE:

   DaaS creates and manages VMs on hosts through those connections. You must specify connections when you create machine catalogs.

Step 2: Prepare master images for your machines

Prepare master images on VMs in your resource location. For more information, see Prepare a master image on the hypervisor or cloud service.

Step 3: Create machine catalogs

Create a machine catalog to create a group of identically configured machines on a host. Detailed steps are as follows:

1. Name the catalog.
2. Select the machine type.

   Options: Multi-session, Single-session static (personal desktops), and Single-session random (pooled desktops).

3. Select a host connection.

   Options originate from all host connections that you've configured for your resource locations in Step 1.

4. Select a master image.
5. Select a machine profile.

   NOTE:

   Machine profile support is currently available for Azure, GCP, and AWS cloud services, and the use of machine profile is optional for GCP.

6. Set how many machines you want to create.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

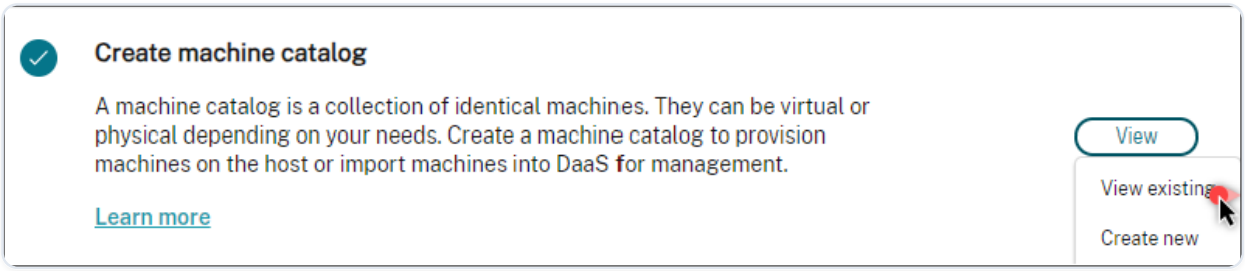
7. Set the machine identities.

   By default, the machine identity type that you selected in the preparation phase is shown. Provide the required identity settings for the VMs, such as domain, OU, and naming scheme.

8. Enter the administrator credentials required for machine creation.
9. Click **Create**.

> **TIP:**
>
> The **Create** button is available only after you provide all required settings.

To view the catalog creation progress, select **View > View existing**.



Step 4: Create delivery groups and assign users

> **TIP:**
>
> Before creating delivery groups, view the existing catalogs to ensure that at least one catalog has been created successfully. Otherwise, you're prevented from creating delivery groups.

Creating a delivery group includes the following subtasks:

- Add VMs to the group
- Assign users to the group
- Specify which apps and desktops you want to make available to assigned users

1. Name the group.
2. Add machines to the group by selecting a machine catalog and specifying how many VMs are available for the group.
3. Specify available applications and desktops for this group:

   - To add applications from a running machine in the selected catalog, click **Add new > From start menu**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To add applications deployed on network shares, click **Add new > Manually**, and then provide the required settings, such as path, working directory, and more.
- (Visible only with multi-session OS machines) For desktop delivery, keep **Enable desktop delivery** selected.

4. Add users who can access apps and desktops in this group.

Step 5: Share the store URL with your users

Go to **StoreFront Cloud \> Access**, and then share the store URL with your users.

Deliver apps and desktops using existing machines (power managed)

This section guides you through the deployment process of delivering apps and desktops using existing machines (power managed).

Prerequisites

Before you start, you need:

- Connectivity from Citrix Cloud to the target identity provider

  For more information, see the corresponding section in Identity providers.
- Role: Full Administrator or Cloud Administrator

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings.

#	SETTING	DESCRIPTION
1	Specify whether VM creation is needed	Select **No**.
2	Select whether power management is required	Select **Machines that are power managed (for example, virtual machines or blade PCs)**.
3	Select the host platform	Select the host platform where your existing machines reside.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING	DESCRIPTION
		Options: AWS, Citrix®, Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis, and VMware
4	Select the user identity type	Select an identity type for user management.
		Options: Active Directory, Microsoft Entra ID, Google Cloud Identity, and Okta

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear. Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location and host connections

Set up your resource location by installing Cloud Connectors and configure connections to hypervisors or cloud services in your location.

1. Name the resource location.
2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.
4. Add and configure host connections for the resource location. Examples of connection settings include the connection address, user name, and password.

NOTE:

DaaS power manages machines in resource locations through connections. You need to specify a connection when importing your machines to a catalog.

Step 2: Create machine catalogs

Create a machine catalog and import your machines to it.

1. Name the catalog

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the machine type.

   Options: Multi-session, Single-session static (personal desktops), and Single-session random (pooled desktops).
3. Select a resource location.
4. Import machines to the catalog. Machines are organized by host connection. Choose a host connection to import associated machines.
5. Click **Create**.

Step 3: Create delivery groups and assign users

To create a delivery group, you must:

- Add VMs to the group
- Assign users to the group
- Specify which apps and desktops you want to make available to assigned users

1. Name the group.
2. Select a machine catalog as needed, and then specify how many machines are available for the delivery group.
3. Specify available applications and desktops for this group:
   - To add applications from a running machine in the selected catalog, click **Add new > From start menu**.
   - To add applications deployed on network shares, click **Add new > Manually**, and then provide the required settings, such as path, working directory, and more.
   - (Visible only with multi-session OS machines) For desktop delivery, keep **Enable desktop delivery** selected.
4. Add users to the group.

Step 4: Share the store URL with your users

Go to **Citrix® StoreFront Cloud \> Access**, and then share the store URL with your users.

Deliver apps and desktops using existing machines (not power-managed)

This section guides you through the deployment process of delivering apps and desktops using existing machines (not power-managed).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

Before you start, you need:

- Connectivity from Citrix Cloud to the target identity provider

  For more information, see the corresponding section in Identity providers
- Role: Full Administrator or Cloud Administrator

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings.

#	SETTING	DESCRIPTION
1	Specify whether VM creation is needed	Select **No**.
2	Select whether power management is required	Select **Machines that are not power managed (for example, physical machines)**.
3	Select the user identity type	Select an identity type for user management.
		Options: Active Directory, Microsoft Entra ID, Google Cloud Identity, and Okta

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear. Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location

Set up your resource location by installing Cloud Connectors.

1. Name the resource location.
2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Creating host connections is required only when you want to power manage machines.

Step 2: Create a machine catalog

Create a machine catalog and import your machines to it.

1. Name the catalog
2. Select the machine type.

   Options: Multi-session, Single-session static (personal desktops), and Single-session random (pooled desktops).
3. Select a resource location.
4. Import machines to the catalog.

   To ease machine search, use partial computer names and directory selection.
5. Click **Create**.

Step 3: Create delivery groups and assign users

To create a delivery group, you must:

- Add VMs to the group
- Assign users to the group
- Specify which apps and desktops you want to make available to assigned users

1. Name the group.
2. Select a machine catalog as needed, and then specify how many machines are available for the delivery group.
3. Specify available applications and desktops for this group:
   - To add applications from a running machine in the selected catalog, click **Add new > From start menu**.
   - To add applications deployed on network shares, click **Add new > Manually**, and then provide the required settings, such as path, working directory, and more.
   - (Visible only with multi-session OS machines) For desktop delivery, keep **Enable desktop delivery** selected.
4. Add users to the group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 4: Share the store URL with your users

Go to **Citrix® StoreFront Cloud \> Access**, and then share the store URL with your users.

Deliver office PCs (power managed)

This section guides you through the deployment process of delivering office PCs (power managed).

Prerequisites

Before you begin, you need:

- Machine names of the PCs.
- Citrix Virtual Delivery Agent (VDA) is installed on each PC. (This step can be done after catalog creation.)

  For more information, see Download VDA.

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings.

#	STEP	DESCRIPTION
1	Select the machine allocation type.	Select how the machines are assigned.
		Options: Static auto-assigned, Static preassigned, and Random pool unassigned
2	Determine whether to allow users to power on machines	Select **I want remote users to power on machines by themselves**.
3	Select the user identity type	Select an identity type for user management.
		Options: Active Directory, Microsoft Entra ID, Google Cloud Identity, and Okta

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear. Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location and host connections

Set up your resource location by installing Cloud Connectors and add a connection of the **Remote PC Wake on LAN** type.

1. Name the resource location.
2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.
4. Click **Add new** to add a connection:
    a. Select a resource location (zone).
    b. Select **Remote PC Wake on LAN** for **Connection type**.
    c. Enter a name for the connection.

NOTE:

DaaS power manages machines through the configured connections. You must configure connections of the **Remote PC Wake on LAN** type when creating Remote PC Access catalogs for power-managed machines.

Step 2: Create a Remote PC Access catalog

Create a machine catalog and import your office PCs to it.

1. Name the catalog
2. Select a resource location.
3. Select a machine allocation type. By default, the type that you selected in the preparation phase is shown.
4. Select the **Wake on LAN connection**. Options are the connections of the **Remote PC Wake on LAN** type that you configured for the selected location.
5. Import your machines.
6. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Create delivery groups and assign users

Create a delivery group to group machines that you want to deliver and specify who can access them.

1. Name the group.
2. Select a machine catalog as needed. Only the **Remote PC Access** catalogs appear.
3. Assign users to the group.

Step 4: Share the store URL with your users

Go to **Citrix® StoreFront Cloud \> Access**, and then share the store URL with your users.

Deliver office PCs (not power-managed)

This section guides you through the deployment process of delivering office PCs (not power-managed).

Prerequisites

Before you begin, you need:

- Machine names of the PCs.
- Citrix Virtual Delivery Agent (VDA) is installed on each PC. (This step can be done after catalog creation.)

  For more information, see Download VDA.

Preparation

Answer the onscreen questions to complete the following infrastructure-level settings.

#	SETTING	DESCRIPTION
1	Select the machine allocation type.	Select how the machines are assigned.
		Options: Static auto-assigned, static preassigned, and random pool unassigned
2	Determine whether to allow users to power on machines	Keep **I want remote users to power on machines by themselves** cleared.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING	DESCRIPTION
3	Select the user identity type	Select an identity type for user management.
		Options: Active Directory, Microsoft Entra ID, Google Cloud Identity, and Okta

Deployment steps

After you complete the infrastructure-level settings, steps specific to this deployment scenario appear. Follow the onscreen instructions to complete the settings.

Step 1: Add a resource location

Set up your resource location by installing Cloud Connectors.

1. Name the resource location.
2. Download and install Cloud Connectors on at least two Windows Server machines.
3. Detect installed Cloud Connectors.

NOTE:

Creating host connections is required only when you want to power manage machines.

Step 2: Create a Remote PC Access catalog

Create a catalog and import your office PCs to it.

1. Name the catalog
2. Select a resource location.
3. Select an allocation type. By default, the type that you selected in the preparation phase is shown.
4. Import your machines.
5. Click **Create**.

Step 3: Create delivery groups and assign users

Create a delivery group for machines that you want to deliver and specify who can access them.

1. Name the group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select a machine catalog as needed. Only the **Remote PC Access** catalogs appear.
3. Assign users for the group.

Step 4: Share the store URL with your users

Go to **Citrix® StoreFront Cloud \> Access**, and then share the store URL with your users.

Machine identities

Each machine must have a unique machine identity, also known as computer account. Machine identities can be created and managed in the machines locally or in a directory, such as on-premises Active Directory (AD) or Microsoft Entra ID. Citrix supports hosting virtual applications and desktops on machines that are Active Directory joined, Microsoft Entra joined, Microsoft Entra hybrid joined, or non-domain joined.

Machine identity types

The following machine identity types are supported.

MACHINE IDENTITY TYPE	DESCRIPTION
AD joined	Identities are created and managed in on-premises Active Directory. Provisioned machines are joined to on-premises Active Directory using the assigned machine identities.
Microsoft Entra joined	Identities are created and managed in Entra ID. Provisioned machines are joined to Entra ID using the assigned machine identities. Importing VMs to Citrix DaaS is not supported.
Microsoft Entra hybrid joined	Identities are created in on-premises Active Directory and are synced with Entra ID through Microsoft Entra Connect. Provisioned machines are joined to on-premises Active Directory and Entra ID. The machines are then Entra hybrid joined. For importing an Entra hybrid joined VM, the VM is treated as an Active Directory joined VM by Citrix DaaS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MACHINE IDENTITY TYPE	DESCRIPTION
Non-domain-joined	Identities are created and managed in the machines locally. Importing VMs to Citrix DaaS is not supported.

Supported Configurations

The following are details of the supported configurations for each scenario.

Supported infrastructure

MACHINE IDENTITY	CITRIX DAAS™	CITRIX® STOREFRONT CLOUD	CITRIX STOREFRONT	CITRIX GATEWAY SERVICE	CITRIX GATEWAY
AD joined	Yes	Yes	Yes	Yes	Yes
Microsoft Entra joined	Yes	Yes	Preview	Yes	No
Microsoft Entra hybrid joined	Yes	Yes	Yes	Yes	Yes
Non-domain-joined	Yes	Yes	Yes	Yes	Yes

NOTE

Neither Local Host Cache nor Service Continuity are available for Non-domain joined session hosts when using Storefront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported Citrix® StoreFront Cloud authentication identity providers

MACHINE IDENTITY	MICROSOFT ENTRA ID	ACTIVE DIRECTORY	ACTIVE DIRECTORY AND TOKEN	OKTA	SAML	CITRIX GATEWAY	ADAPTIVE AUTHENTICATION
AD joined	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Entra joined	Yes	No	No	No	Yes	No	No
Microsoft Entra hybrid joined	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Non-domain-joined	Yes	Yes	Yes	Yes	Yes	Yes	Yes

NOTE

- If using an identity provider other than Active Directory or Active Directory + Token with AD joined or Entra hybrid joined deployments, you need Citrix Federated Authentication Service (FAS) to achieve single sign-on (SSO) to the virtual app or desktop session. Refer to the FAS documentation for details.

If you plan to use SAML as your identity provider and require access to Microsoft Entra joined session hosts, see the Citrix Cloud documentation for information on configuring SAML with Entra ID identities.

Active Directory joined

Identities are created and managed in on-premises Active Directory. Provisioned machines are joined to on-premises Active Directory using the assigned machine identities. For more information on supported functional levels for the forest and domain, see Active Directory functional levels.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For information on how to create identity pool of on-premises Active Directory (AD) joined machine identity using Citrix DaaS, see Identity pool of on-premises Active Directory joined machine identity.

Microsoft Entra joined

This article describes the requirements to create Microsoft Entra joined catalogs using Citrix DaaS™ in addition to the requirements outlined in the Citrix DaaS system requirements section.

Requirements

- Control plane: See Supported Configurations
- VDA type: Single-session (desktops only) or multi-session (apps and desktops)
- VDA version: 2203 or later
- Provisioning type: Machine Creation Services™ (MCS), Persistent and Non-persistent using Machine Profile workflow
- Assignment type: Dedicated and pooled
- Hosting platform: Azure only
- Rendezvous V2 must be enabled
- Single sign-on: See Microsoft Entra single sign-on for DaaS

Limitations

- Service continuity is not supported.
- Logging in with Windows Hello in the virtual desktop is only supported with PIN. Biometric authentication methods (facial recognition, fingerprint recognition, and iris recognition) are not supported at this time.
- Support only Microsoft Azure Resource Manager cloud environments.
- If single sign-on is disabled, the first time a virtual desktop session is launched, the Windows sign-in screen may show the logon prompt for the last logged on user without the option to switch to another user. The user must wait until the logon times out and the desktop's lock screen appears, and then click the lock screen to reveal the logon screen once again. At this point, the user is able to select **Other Users** and enter their credentials. This is the behavior with every new session when the machines are non-persistent.
- When multiple machine catalogs are joined to the same Azure tenant, each catalog must use a unique `NamingScheme`. If different catalogs use the same `NamingScheme`, VMs might be created with duplicate names, which causes the Entra ID join to fail due to name conflicts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Considerations

Image configuration

- Consider optimizing your Windows image using the Citrix Optimizer tool.

Microsoft Entra joined

- Consider disabling Windows Hello so users are not prompted to set it up when they log into their virtual desktop. If you are using VDA 2209 or later, this is done automatically. For earlier versions, you can do this in one of two ways:
  - Group policy or local policy
    - Navigate to **Computer Configuration > Administrative Templates > Windows Components > Windows Hello for Business**.
    - Set **Use Windows Hello for Business** to:
      - **Disabled**, or
      - **Enabled** and select **Do not start Windows Hello provisioning after sign-in**.
  - Microsoft Intune
    - Create a device profile that disables Windows Hello for Business. Refer to Microsoft documentation for details.
- Users must be granted explicit access in Azure to log into the machines using their Microsoft Entra credentials. This can be facilitated by adding the role assignment at the resource group level:
  a. Sign into the Azure portal.
  b. Select **Resource Groups**.
  c. Click the resource group where the virtual desktop workloads reside.
  d. Select **Access control (IAM)**.
  e. Click **Add role assignment**.
  f. Search for **Virtual Machine User Login**, select it on the list, and click **Next**.
  g. Select **User, group, or service principal**.
  h. Click **Select members** and select the users and groups you want to provide access to the virtual desktops.
  i. Click **Select**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

j. Click **Review + assign**.

k. Click **Review + assign** once again.

NOTE:

If you choose to let MCS create the resource group for the virtual desktops, you add this role assignment after the machine catalog is created.

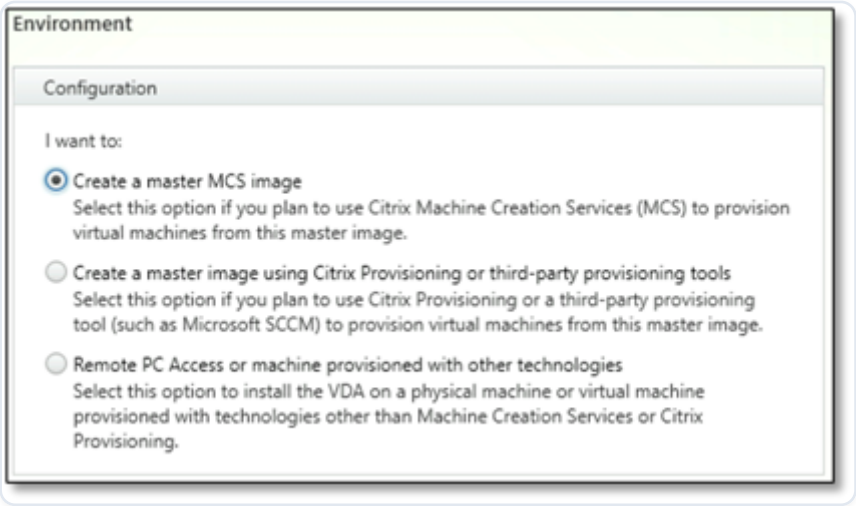
- Master VMs can be Microsoft Entra joined or non-domain-joined. This functionality requires VDA version 2212 or later.

VDA installation and configuration

Follow the steps for installing the VDA:

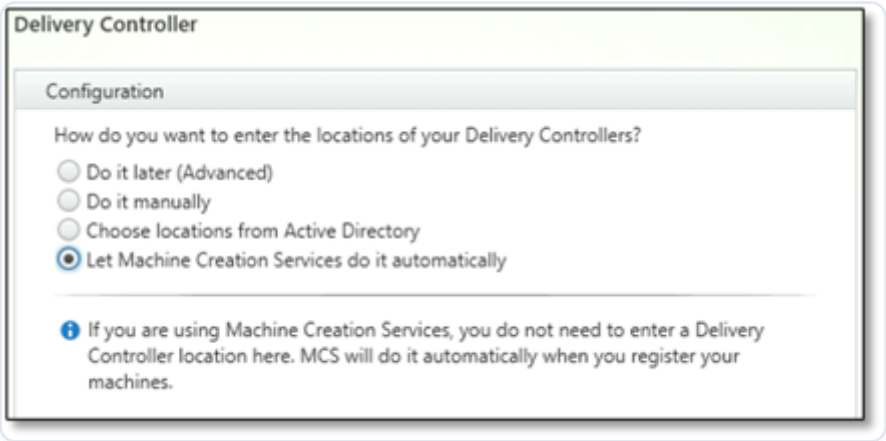
1. Make sure to select the following options in the installation wizard:

   - In the Environment page, select **Create a master MCS image**.



   - In the Delivery Controller™ page, select **Let Machine Creation Services do it automatically**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. (Only for VDA versions earlier than 2311) After the VDA is installed, add the following registry value:

   - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Value type: DWORD
   - Value name: GctRegistration
   - Value data: 1

3. For Windows 11 22H2 based master VM, create a scheduled task in the master VM that executes the following command at system startup using SYSTEM account. This task of scheduling a task in the master VM is only required for VDA version 2212 or earlier.

   ```
   reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ /d Citrix /f
   ```

4. If you join the master VM to Microsoft Entra ID, and then manually remove the join by `dsregcmd` utility, make sure that the value of `AADLoginForWindowsExtensionJoined` under HKLM\Software\Microsoft\Windows Azure\CurrentVersion\AADLoginForWindowsExtension is zero.

Where to go next

Once the resource location and hosting connection are available, proceed to create the machine catalog. For more information on creating identity pool of Microsoft Entra joined machine identity, see Identity pool of Microsoft Entra joined machine identity.

Microsoft Intune

This article describes the requirements to create Microsoft Intune enabled catalogs using Citrix DaaS™ in addition to the requirements outlined in the Citrix DaaS system requirements section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). You control how your organization's devices are used, including mobile phones, tablets, and laptops. For more information, see Microsoft Intune. The devices must meet the minimum system requirements. For more information, see the Microsoft documentation Supported operating systems and browsers in Intune.

IMPORTANT:

Before enabling this feature, verify that your Azure environment meets the licensing requirements to use Microsoft Intune. For more information, see the Microsoft documentation: `<https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses>`. Do not enable the feature if you do not have the appropriate Intune license.

You can create:

- Microsoft Entra joined catalogs enrolled in Microsoft Intune for persistent and non-persistent, single-session and multi-session VMs. For requirements, limitations, and considerations, see Requirements for Microsoft Entra joined catalogs enrolled in Microsoft Intune.
- Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune for persistent single and multi-session VMs using device credential with co-management capability. For requirements, limitations, and considerations, see Requirements for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune. You can also create Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune for non-persistent single and multi-session VMs. However, this is currently under Preview. See Enrollment of Hybrid Entra ID joined non-persistent VMs into Microsoft Intune.

Requirements for Microsoft Entra joined catalogs enrolled in Microsoft Intune

- Control plane: Citrix DaaS
- VDA type: Single-session and multi-session OS VDA
- VDA version

TYPE OF CATALOG	VDA VERSION
Microsoft Entra joined catalogs enrolled in Microsoft Intune for persistent, single and multi-session VMs	2203 and later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE OF CATALOG	VDA VERSION
Microsoft Entra joined catalogs enrolled in Microsoft Intune for non-persistent, single-session and multi-session VMs	2407 and later

- Provisioning type: Machine Creation Services™ (MCS) persistent and non-persistent machine catalogs using the Machine Profile workflow only

Limitations for Microsoft Entra joined catalogs enrolled in Microsoft Intune

- Do not skip image preparation while creating or updating machine catalogs.

Considerations for Microsoft Entra joined catalogs enrolled in Microsoft Intune

- Create a device profile that disables Windows Hello for Business.
- Use VDA version 2212 or later if Microsoft Intune must manage a master VM.
- Configure Microsoft Intune to delete the stale devices. This ensures that your device records stay current. For information on deleting the stale devices, see Automatically delete devices with cleanup rules.

Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune

Microsoft Entra hybrid joined catalogs, persistent single and multi-session VMs, enrolled in Microsoft Intune use the device credentials with co-management capability.

Co-management enables you to concurrently manage Windows 10 or later devices by using both Configuration Manager and Microsoft Intune. For more information, see Co-management.

Prerequisites for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune

Before enabling this feature, verify that:

- Your Azure environment meets the licensing requirements to use Microsoft Intune. For more information, see the Microsoft documentation.
- You have a valid Configuration Manager deployment with co-management enabled. For more information, see the Microsoft documentation.

Requirements for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune

- Control plane: Citrix DaaS
- VDA type: Single-session or multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VDA version: 2407 or later
- Provisioning type: Machine Creation Service (MCS), Persistent
- Assignment type: Dedicated and pooled
- Hosting platform: Any hypervisor or cloud service

Limitations for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune

- Do not skip image preparation while creating or updating machine catalogs.
- Internet-based client management (IBCM) of Configuration Manager is not supported.

Considerations for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune

- Intune enrollment might be delayed if too many machines in the catalog are powered on simultaneously.

  Microsoft imposes a per-tenant Intune enrollment restriction that limits the number of devices that can be enrolled within a specific time frame. The allowable number of devices varies depending on the number of Microsoft Intune licenses associated with the tenant. Consult your Microsoft account team to find out the allowable limit for your tenant. This approach helps Microsoft Intune enrollment scale better for large environments.

  For persistent machines, there might be an initial wait time required for all devices to complete Intune enrollment.
- Configure Cloud Attach of Configuration Manager. For more information, see the Microsoft documentation.
- Manually install Configuration Manager client on the master VM without assigning the site code with `.\CCMSetup.exe /mp:SCCMServer /logon FSP=SCCMServer`. The SCCMServer is the SCCM server name in your environment. For more information, see the Microsoft documentation.
- MCS created machines use the automatic site assignment mechanism to find site boundary groups that are published to Active Directory Domain Services. Ensure that the boundaries and boundary groups of **Configuration Manager** are configured in your environment. If automatic site assignment is not available, a static Configuration Manager site code can be configured in the master VM through the following registry setting:

  Key:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MachineIdentityServiceAgent\DeviceMa
nagement
```

Value name: `MdmSccmSiteCode`

Value type: **String**

Value data: `the site code to be assigned`

- Configure Microsoft Intune to delete the stale devices. This ensures that your device records stay current. For information on deleting the stale devices, see Automatically delete devices with cleanup rules.

Where to go next

- For information on creating an identity pool of Microsoft Intune enabled machine identity, see Identity pool of Microsoft Intune enabled machine identity.

Microsoft Entra hybrid joined

This article describes the requirements to create Microsoft Entra hybrid joined joined catalogs using Citrix DaaS in addition to the requirements outlined in the Citrix DaaS system requirements section.

This article describes the requirements to create Hybrid Azure Active Directory (HAAD) joined catalogs using Citrix DaaS™ in addition to the requirements outlined in the Citrix DaaS system requirements section.

Hybrid Azure AD joined machines use on-premises AD as the authentication provider. You can assign them to domain users or groups in on-premises AD. To enable Azure AD seamless SSO experience, you need to have the domain users synced to Azure AD.

NOTE:

Microsoft Entra hybrid joined VMs are supported in both federated and managed identity infrastructures.

Requirements

- Control plane: See Supported Configurations
- VDA type: Single-session (desktops only) or multi-session (apps and desktops)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VDA version: 2212 or later
- Provisioning type: Machine Creation Services™ (MCS), Persistent and Non-persistent
- Assignment type: Dedicated and pooled
- Hosting platform: Any hypervisor or cloud service

Limitations

- If Citrix Federated Authentication Service (FAS) is used, single sign-on is directed to on-premises AD rather than Microsoft Entra ID. In this case, it is recommended to configure Microsoft Entra certificate-based authentication so that the primary refresh token (PRT) is generated upon user logon, which facilitates single sign-on to Microsoft Entra resources within the session. Otherwise, the PRT will not be present and SSO to Microsoft Entra resources will not work. For information on achieving Microsoft Entra single sign-on (SSO) to hybrid joined VDAs using Citrix Federated Authentication Service (FAS), see Hybrid-joined VDAs.
- Do not skip image preparation while creating or updating machine catalogs. If you want to skip image preparation, make sure the master VMs are not Microsoft Entra or Microsoft Entra hybrid joined.

Considerations

- Creating Microsoft Entra hybrid joined machines requires the `Write userCertificate` permission in the target domain. Make sure that you enter credentials of an administrator with that permission during catalog creation.
- The hybrid Microsoft Entra joining process is managed by Citrix. You need to disable `autoWorkplaceJoin` controlled by Windows in the master VMs as follows. The task of manually disabling `autoWorkplaceJoin` is only required for VDA version 2212 or earlier.

  a. Run `gpedit.msc`.

  b. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Device Registration**.

  c. Set **Register domain joined computers as devices** to **Disabled**.

- Select the Organizational Unit (OU) that is configured to be synced with Microsoft Entra ID when you create the machine identities.
- For Windows 11 22H2 based master VM, create a scheduled task in the master VM that executes the following commands at system startup using SYSTEM account. This task of scheduling a task in the master VM is only required for VDA version 2212 or earlier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'

$WorkplaceJoinKeyPath = 'HKLM:
\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin'

$MaxCount = 60



for ($count = 1; $count -le $MaxCount; $count++)

{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)

  {

    $provider = (Get-Item -Path
$VirtualDesktopKeyPath).GetValue("Provider", $null)

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "Provider"
-Value "Citrix" -Force

        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name
"autoWorkplaceJoin" -Value 1 -Force

        Start-Sleep 5

        dsregcmd /join
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        break

    }

  }



  Start-Sleep 1

}
```

- By default, Microsoft Entra Connect synchronizes every 30 minutes. The provisioned machines can take up to 30 minutes to be Microsoft Entra hybrid joined during the first boot.

Where to go next

For more information on creating identity pool of Microsoft Entra hybrid joined machine identity, see Identity pool of Microsoft Entra hybrid joined machine identity.

Non-domain-joined

This article describes the requirements to create non-domain-joined catalogs using Citrix DaaS™ in addition to the requirements outlined in the Citrix DaaS system requirements section.

Requirements

- Control plane: See Supported Configurations
- VDA type: Single-session (desktops only) or multi-session (apps and desktops)
- VDA version: 2203 or later
- Provisioning type: Machine Creation Services™ (MCS), Persistent and Non-persistent
- Assignment type: Dedicated and pooled
- Hosting platform: All platforms supported by MCS
- Rendezvous V2 must be enabled
- Cloud Connectors: Only required if you plan to provision machines on on-premises hypervisors or if you want to use Active Directory as the identity provider in Workspace.

Limitations

- Service continuity is not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

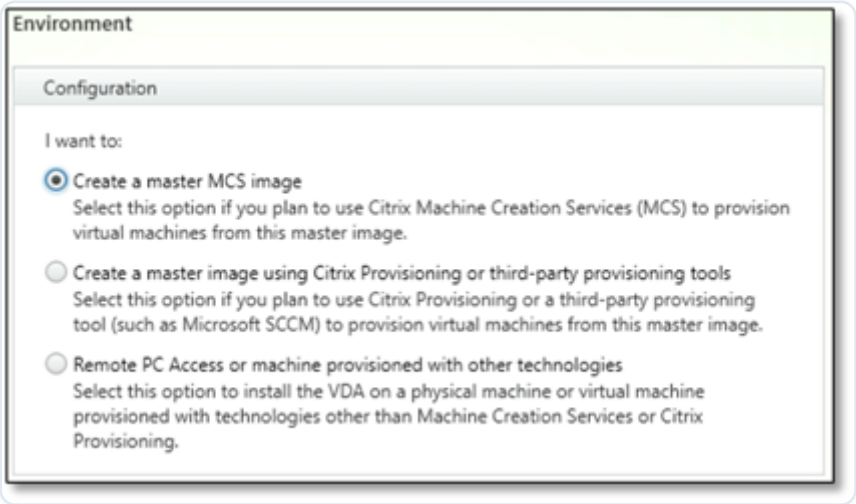
- Whenever we use a multi session non domain joined VDA, the local user's profile data is not retained and is deleted on logoff.

VDA installation and configuration

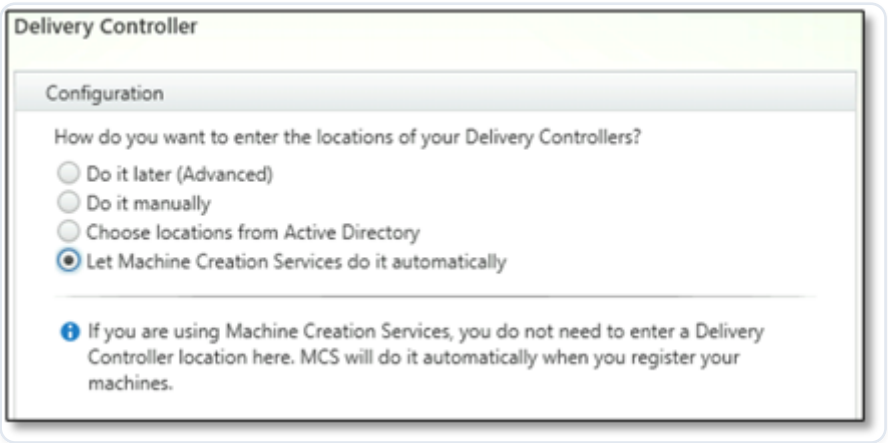
Follow the steps for installing the VDA:

1. Make sure to select the following options in the installation wizard:

    - In the Environment page, select **Create a master MCS image**.



    - In the Delivery Controller™ page, select **Let Machine Creation Services do it automatically**.



2. After the VDA is installed, add the following registry value:

    - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
    - Value type: DWORD
    - Value name: GctRegistration
    - Value data: 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Where to go next

Once the resource location and hosting connection are available, proceed to create the machine catalog. For more information on creating identity pool of non-domain-joined machine identity, see Identity pool of non-domain-joined machine identity.

Session authentication

Citrix supports multiple methods for authenticating users into virtual desktop and application sessions. The available options depend on how your environment is configured; specifically, the directory service where user accounts reside (e.g. Active Directory or Microsoft Entra ID), the directory service where the session host machines are joined, and the identity provider used for initial logon into the Citrix environment. These factors determine whether authentication can be handled through traditional credentials, smart cards, federated assertions, or certificate-based mechanisms. This section outlines the available authentication methods and how they align with different deployment scenarios.

Microsoft Entra single sign-on

You can leverage single sign-on (SSO) when using Microsoft Entra ID credentials to access virtual applications and desktops on Microsoft Entra joined or Microsoft Entra hybrid joined session hosts.

Supported infrastructure

The following is an overview of the infrastructure components supported for Microsoft Entra single sign-on:

MACHINE IDENTITY	CITRIX DAAS	CITRIX DAAS LOCAL	CITRIX STOREFRONT CLOUD	CITRIX STOREFRONT	CITRIX GATEWAY SERVICE	NETSCALER GATEWAY
Microsoft Entra joined	Yes	No	Yes	No	Yes	Yes
Microsoft Entra hybrid joined	Yes	Yes	Yes	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- For details on configuring Microsoft Entra single sign-on with **Citrix DaaS Local**, refer to the Citrix DaaS Local documentation.
- For details on configuring Microsoft Entra single sign-on with **StoreFront**, refer to the StoreFront documentation.

Supported identity providers

The following is an overview of the Workspace identity providers supported for Microsoft Entra single sign-on:

MACHINE IDENTITY	ENTRA ID	ACTIVE DIRECTORY	ACTIVE DIRECTORY + TOKEN	OKTA	SAML	NETSCALER GATEWAY	ADAPTIVE AUTHENTICATION
Microsoft Entra joined	Yes	No	No	No	Yes	No	No
Microsoft Entra hybrid joined	Yes	No	No	No	Yes	No	No

NOTE

If you are planning to use SAML as your IdP, you must ensure your SAML provider is configured properly to support Entra based authentication. See SAML using Microsoft Entra ID and Microsoft Entra identities for workspace authentication.

Supported access methods

The following are the access methods available in a Citrix environment:

- **Native access:** You use the native Citrix Workspace app client to access your store and establish the session connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Browser access:** You access your store through a browser and connect to the virtual app or desktop session using the Citrix Workspace app for HTML5 client.
- **Hybrid access:** You access your store through a browser and connect to the virtual app or desktop session using the native Workspace app client.

The following is an overview of the access methods supported for Microsoft Entra single sign-on:

ACCESS METHOD	WINDOWS	LINUX	MAC	CHROME OS	ANDROID	IOS
Native	Yes	Yes	Yes	Yes	Yes	Yes
Browser	Yes	Yes	Yes	Yes	Yes	Yes
Hybrid	Yes	Yes	Yes	No	No	No

System requirements

The following are the system requirements for using Microsoft Entra single sign-on:

- Control plane: Citrix DaaS
  - Citrix Cloud Commercial (US, EU, and APS)
  - Citrix Cloud Japan
- User portal: Citrix® StoreFront Cloud
- Virtual Delivery Agent (VDA)
  - Windows: version 2507 or newer
- Citrix Workspace app
  - Windows: version 2507 or newer
  - Linux: version 2508 or newer (version 2601 or newer required for hybrid access)
  - Mac: version 2508 or newer (version 2511 or newer required for hybrid access)
  - HTML5: version 2511 or newer
  - Chrome OS: version 2511 or newer
  - Android: version 2511 or newer
  - iOS: version 2511 or newer
- Citrix Web Extension

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - Microsoft Edge
  - Google Chrome

- Session host OS:
  - Windows 11, version 24H2 with 2025-09 Cumulative Updates for Windows 11 (KB5065789) or later installed (build 26100.6725)
  - Windows Server 2025 with 2026-01 Cumulative Updates for Windows Server 2025 (KB5073379) or later installed (build 26100.32230)

NOTE

The Citrix Web Extension is only needed if your users will be leveraging hybrid access in **Windows**, **Linux**, or **Mac** devices. If your users leverage native or browser access, the Citrix Web Extension is not needed.

Considerations

- If your users will be leveraging hybrid access, they must use either Microsoft Edge or Google Chrome, and install the Citrix Web Extension. Microsoft Entra single sign-on with hybrid access is not supported with other browsers.
- Auto Client Reconnect is not supported when Microsoft Entra single sign-on is used to log into the session. This feature is automatically disabled when this logon method is used. Session Reliability is still available for automatic reconnection in case of network disruptions.
- When a virtual desktop is locked, the default behavior is to display the Windows lock screen. Depending on your authentication requirements, you might need to change the session lock behavior. See Session lock behavior for more details.
- If using Microsoft Entra hybrid joined session hosts, single sign-on does not work by default for members of privileged groups such as Domain Admins. To enable it, add the group or user to the Read-Only Domain Controller (RODC) allowlist for Microsoft Entra Kerberos access. See Microsoft Entra Kerberos TGT and Active Directory access control for details.
- Microsoft Entra External ID is not supported at this time. If you need to provide access to guest users, refer to SAML using Entra ID for Guest and B2B identities for workspace authentication.
- Microsoft Entra single sign-on requires the Windows setting **Allow Custom SSPs and APs to be loaded into LSASS** to be enabled (default). Note that if you deploy the **Security Baseline for Windows 10 and later** template via Microsoft Intune, this setting is automatically disabled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

and will block SSO, so you must update your Intune device configuration policy to keep it enabled.

How to configure Microsoft Entra single sign-on

Overview

The configuration of Microsoft Entra single sign-on consists of the following steps:

1. Azure and Microsoft Entra ID configuration
    a. Register the Citrix resource and client applications.
    b. Enable the Microsoft Entra ID Remote Desktop Services authentication protocol for the Citrix resource application.
    c. Hide the user consent prompt.
    d. Approve the client application.
    e. Create a Kerberos server object (Microsoft Entra hybrid joined environments only).
    f. Review Microsoft Entra Conditional Access policies.
2. Citrix configuration
    a. Provision session hosts with the required OS version, identity type, and VDA version.
    b. Configure Citrix® StoreFront Cloud:
        i. Configure an appropriate Identity Provider.
        ii. Enable Microsoft Entra single sign-on
    c. Configure your Delivery Groups' logon type if needed.

Details of each configuration step are provided in the sections that follow.

Azure and Microsoft Entra ID configuration

In order to leverage Microsoft Entra single sign-on, you must first allow Microsoft Entra authentication for Windows in your Microsoft Entra ID tenant, which enables issuing the required authentication tokens that allow users to sign in to the Microsoft Entra joined and Microsoft Entra hybrid joined session hosts.

The person making the Azure configuration must be assigned one of the following Microsoft Entra built-in roles or equivalent at a minimum:

- Application Administrator

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cloud Application Administrator

The configuration can be completed through Azure Portal, using Microsoft Graph PowerShell SDK, or Microsoft Graph API. The following sections provide details for completing the configuration through Azure Portal. If you prefer to use Microsoft Graph PowerShell SDK or Microsoft Graph API, refer to Microsoft Entra single sign-on Azure configuration.

REGISTER CITRIX APPLICATIONS

Microsoft Entra single sign-on requires an Entra ID Resource Application and an Entra ID Client Application. The Resource Application represents the Windows OS when requesting the RDP Access Token. The Client Application represents the Citrix Workspace app.

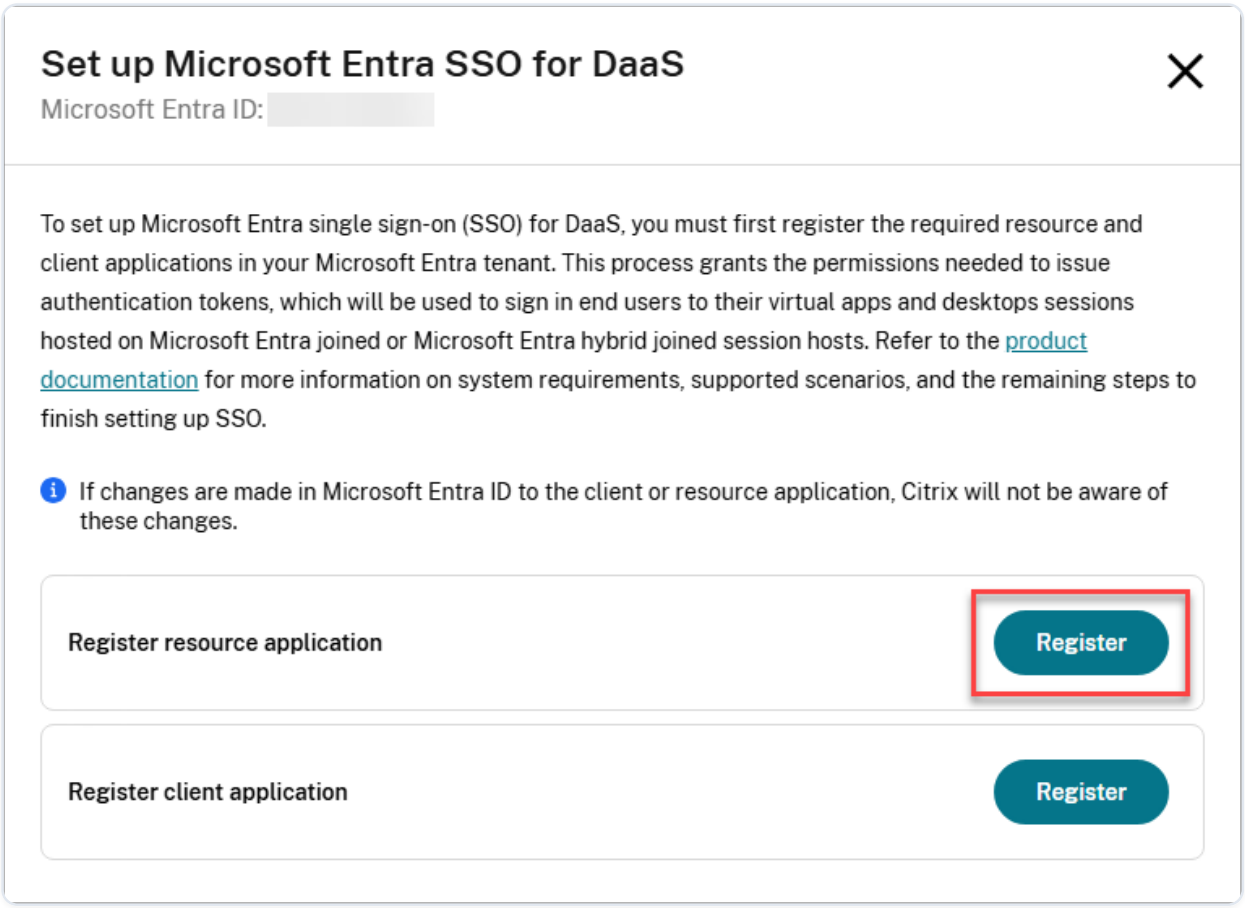
You can register the Citrix Resource and Citrix Client applications through the **Citrix Cloud portal**:

1. Open the menu on the upper left corner and select `Identity and access management`.
2. In the `Authentication` page, look for the Microsoft Entra ID identity provider for which you want to enable Microsoft Entra single sign-on.
3. Open the options menu and select `Set up Microsoft Entra SSO`.



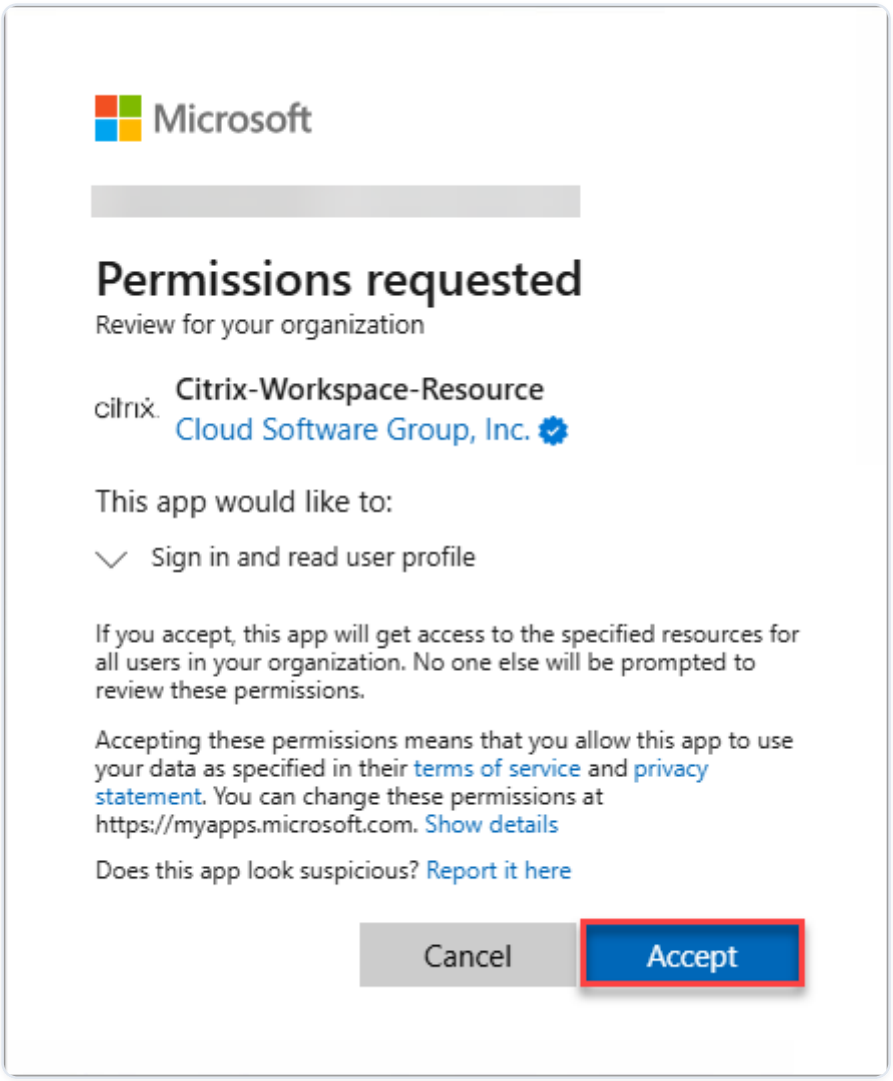
4. Click on `Register` next to **Register resource application**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



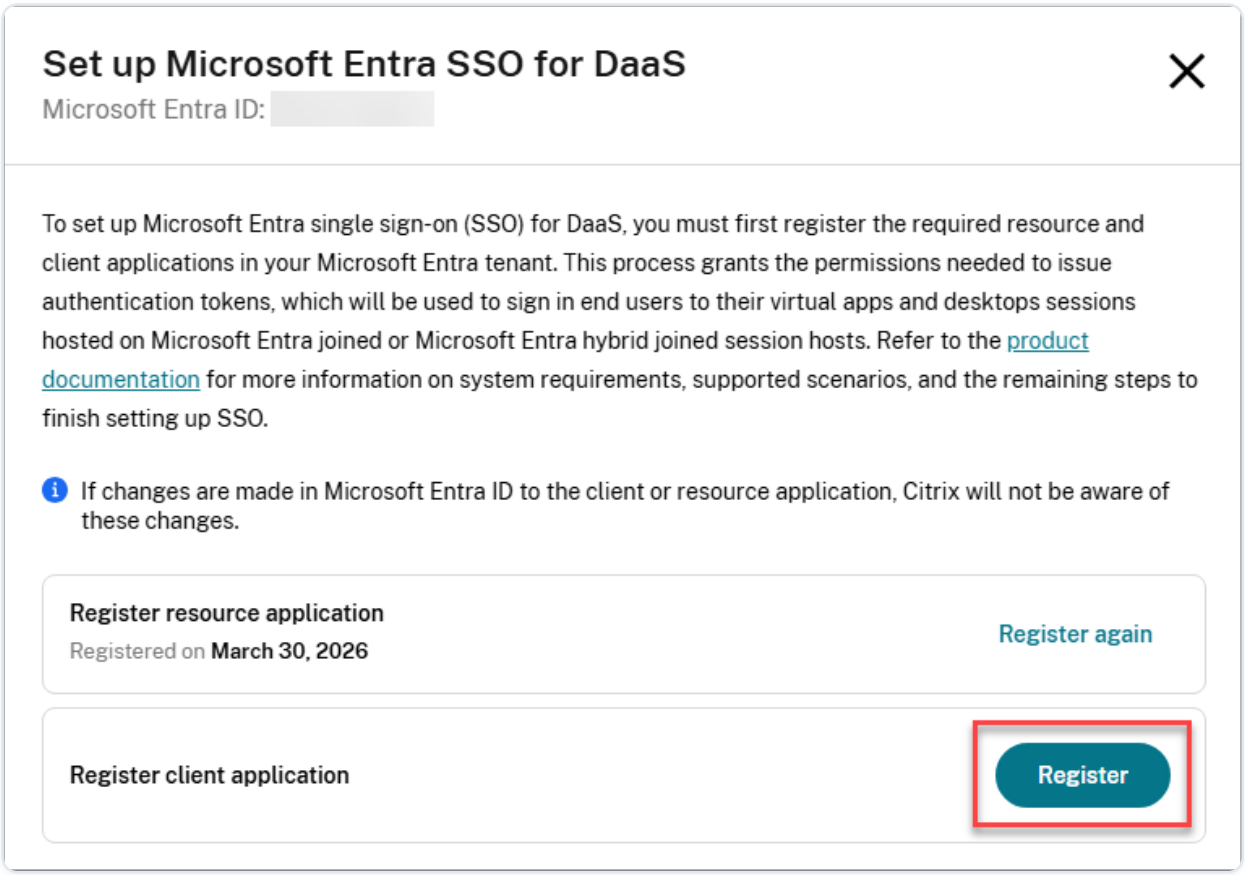
5. Accept the permissions requested for the Citrix Resource application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

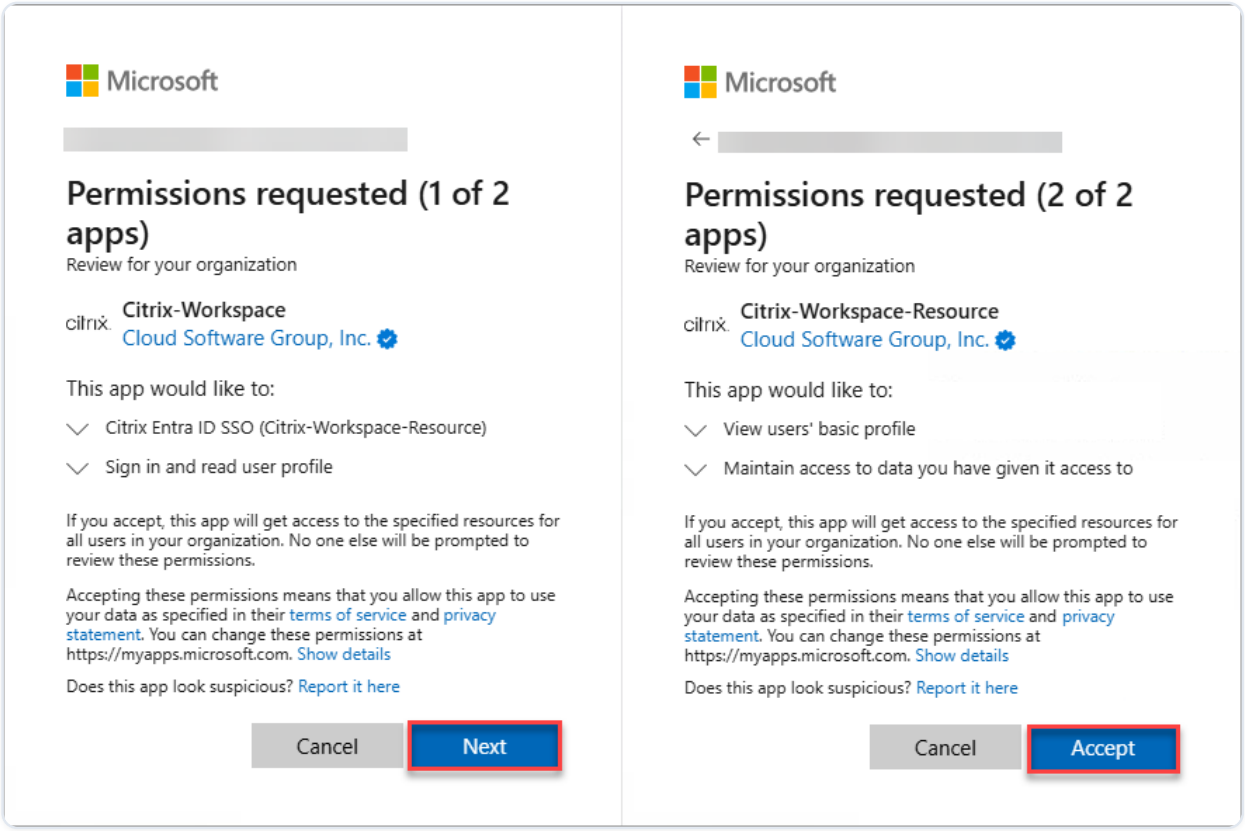


6. Click on `Register` next to **Register client application**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. Accept the permissions requested for the Citrix Client application.



Alternatively, you can use the following consent URLs to register the applications. Please make sure to register the Resource app first, followed by the Client app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Cloud US, EU, APS
  - Resource app: `https://login.microsoftonline.com/common/adminconsent?client_id=3a510bb1-e334-4298-831e-3eac97f8b26c`
  - Client app: `https://login.microsoftonline.com/common/adminconsent?client_id=85651ebe-9a8e-49e4-aaf2-9274d9b6499f`
- Citrix Cloud Japan
  - Resource app: `https://login.microsoftonline.com/common/adminconsent?client_id=0027603f-364b-40f2-98be-8ca4bb79bf8b`
  - Client app: `https://login.microsoftonline.com/common/adminconsent?client_id=0fa97bc0-059c-4c10-8c54-845a1fd5a916`

The following are the applications' permissions:

Citrix Resource application

A service principal is created with the following permissions:

API NAME	CLAIM VALUE	PERMISSION	TYPE
Microsoft Graph	User.Read	Sign in and read user profile	Delegated

For Citrix Cloud US, EU, and APS, the application is called Citrix-Workspace-Resource (application ID 3a510bb1-e334-4298-831e-3eac97f8b26c).

For Citrix Cloud Japan, the application is called Citrix-Workspace-Resource-JP (application ID 0027603f-364b-40f2-98be-8ca4bb79bf8b).

Citrix Client application

A service principal is created with the following permissions:

API NAME	CLAIM VALUE	PERMISSION	TYPE	
Citrix-Workspace-Resource Citrix-Workspace-Resource-JP	user_impersonation	Citrix Entra ID SSO	Delegated	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

API NAME	CLAIM VALUE	PERMISSION	TYPE
Microsoft Graph	User.Read	Sign in and read user profile	Delegated

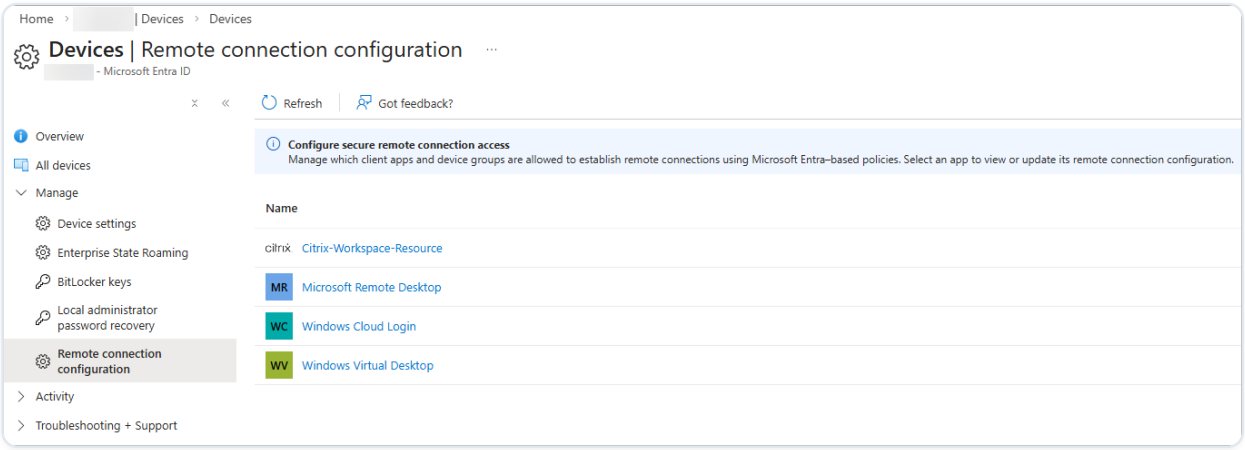
For Citrix Cloud US, EU, and APS, the application is called Citrix-Workspace (application ID 85651ebe-9a8e-49e4-aaf2-9274d9b6499f).

For Citrix Cloud Japan, the application is called Citrix-Workspace-JP (application ID 0fa97bc0-059c-4c10-8c54-845a1fd5a916).

ENABLE MICROSOFT ENTRA ID REMOTE DESKTOP SERVICES AUTHENTICATION PROTOCOL

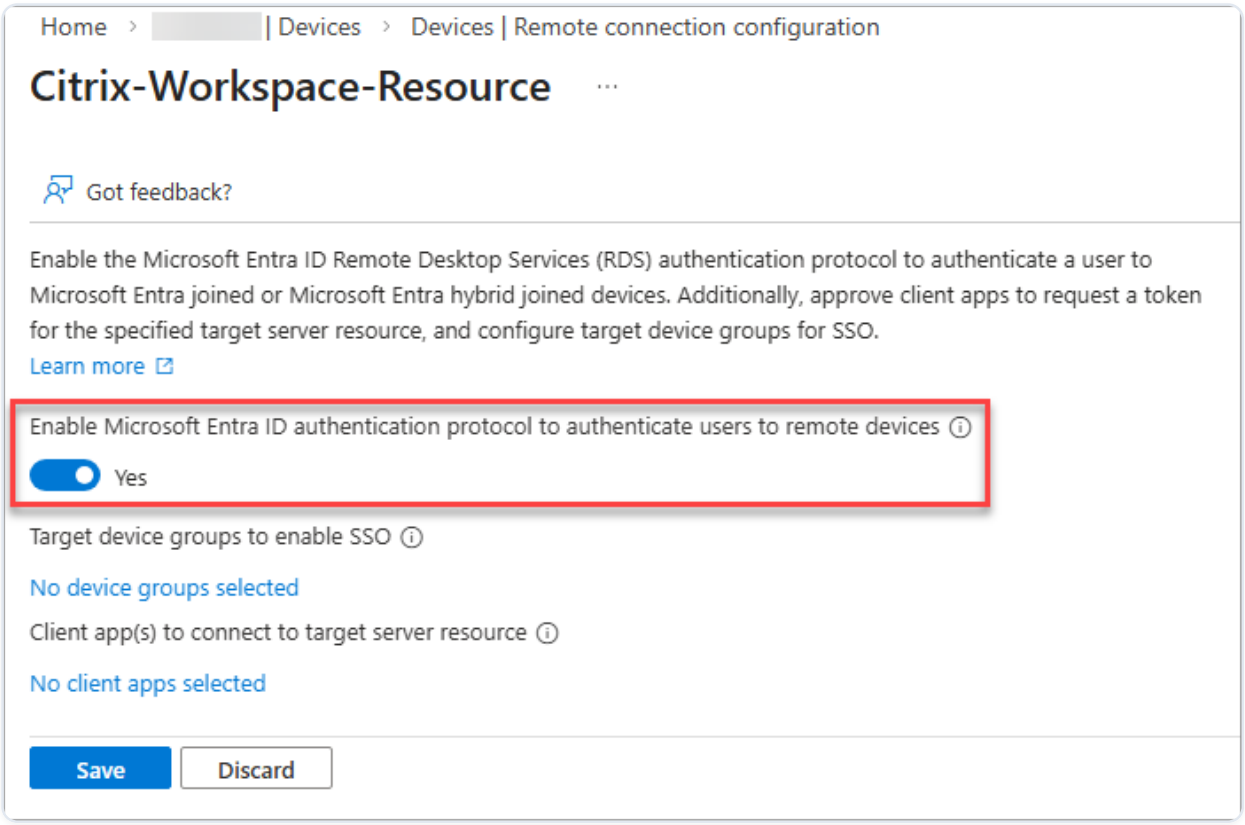
You must enable the Microsoft Entra ID Remote Desktop Services authentication protocol in the Citrix Resource application. To do so:

1. In Azure Portal, navigate to `Microsoft Entra ID` > `Devices` > `Manage` > `Remote connection configuration`.



2. Select **Citrix-Workspace-Resource**.
3. Enable **Microsoft Entra ID Remote Desktop Services authentication protocol**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Proceed to hide the user consent prompt.

HIDE THE USER CONSENT PROMPT DIALOG

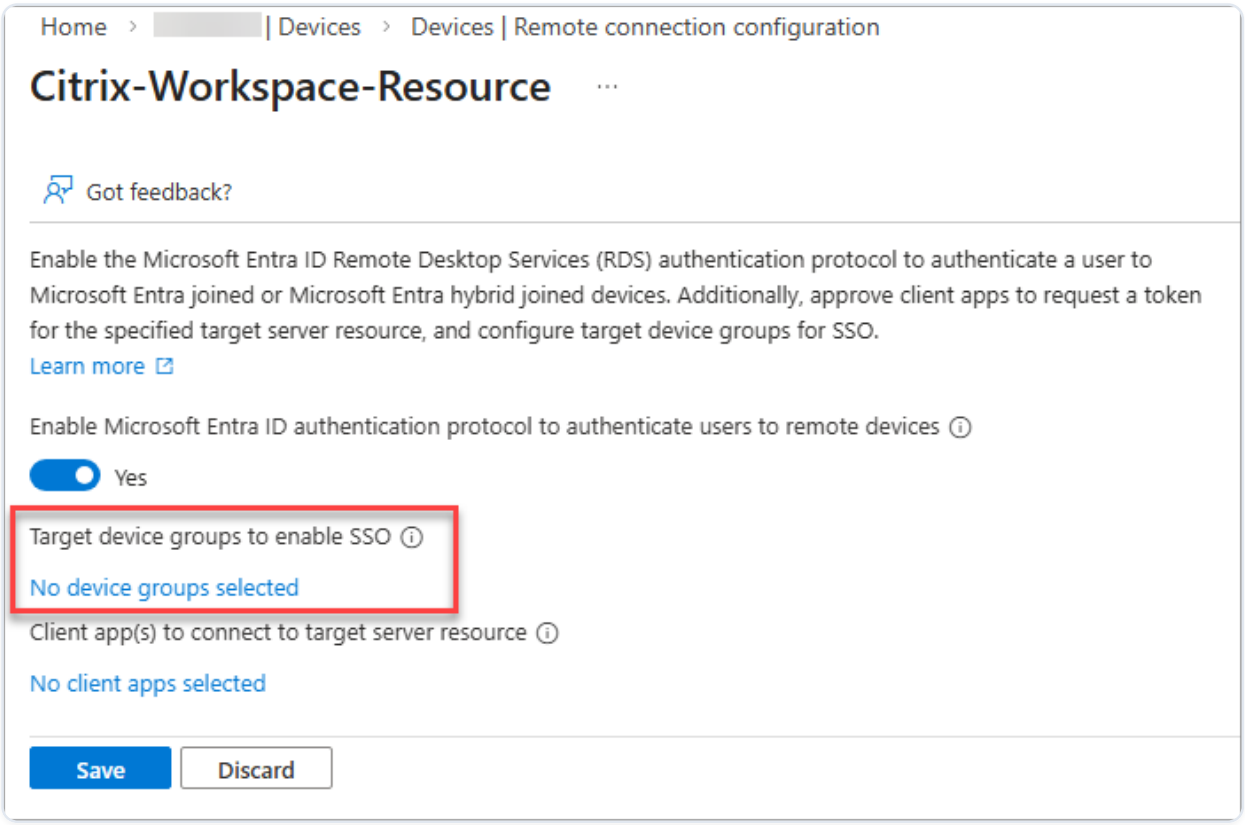
By default, users are prompted to allow the Remote Desktop connection when connecting to a Microsoft Entra joined or Microsoft Entra hybrid joined session host with Microsoft Entra single sign-on enabled, in which they must select **Yes** to allow single sign-on. Microsoft Entra will remember up to 15 unique session hosts for 30 days before prompting again.

You can hide this dialog by configuring a list of target devices. To configure the list of devices, you must create one or more groups in Microsoft Entra ID that contain the Microsoft Entra joined and/or Microsoft Entra hybrid joined session hosts and then authorize the groups in the resource application, up to a maximum of 10 groups.

Once you have enabled the Microsoft Entra ID Remote Desktop Services authentication protocol and the groups have been created:

1. Click on the link to add the target device groups and select the appropriate groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

It is highly recommended to create a dynamic group to simplify the membership management for the group. While dynamic groups normally update within 5-10 minutes, large tenants can take up to 24 hours.

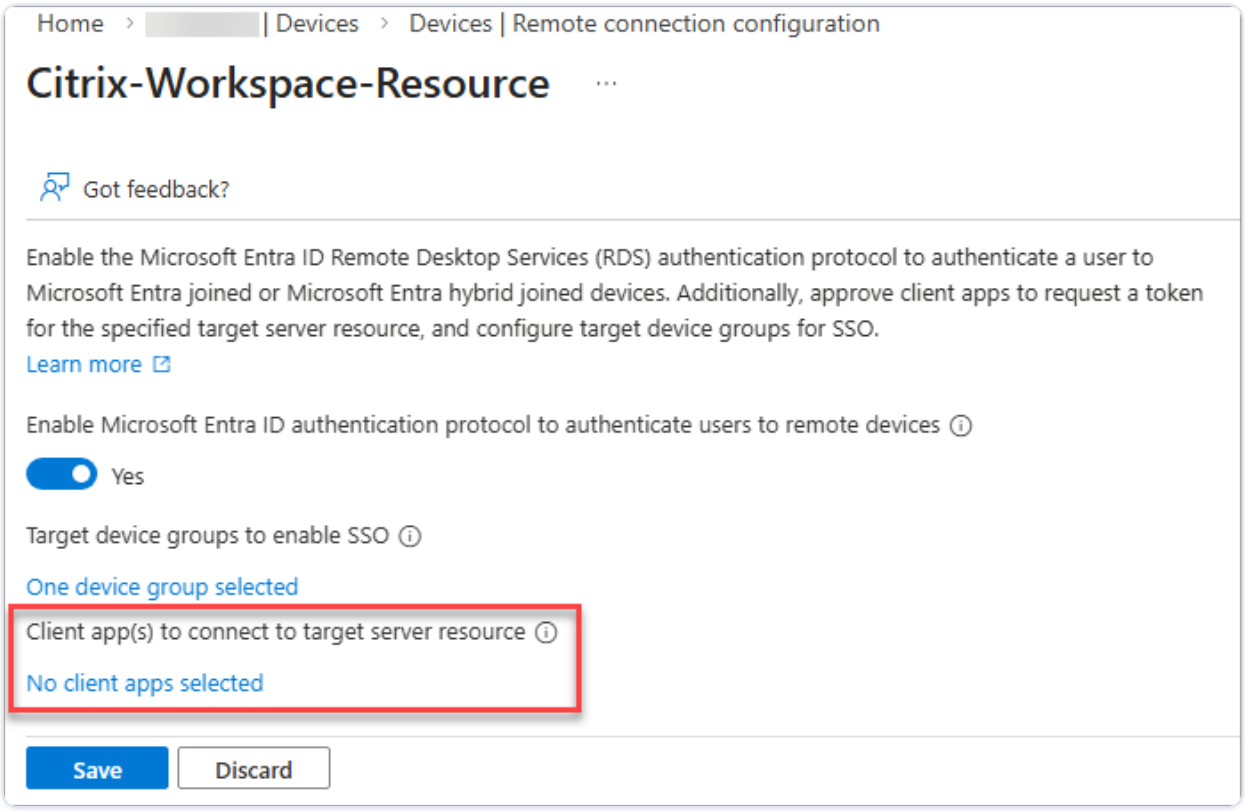
Dynamic groups requires the Microsoft Entra ID P1 license or Intune for Education license. For more information, see Dynamic membership rules for groups.

APPROVE THE CLIENT APPLICATION

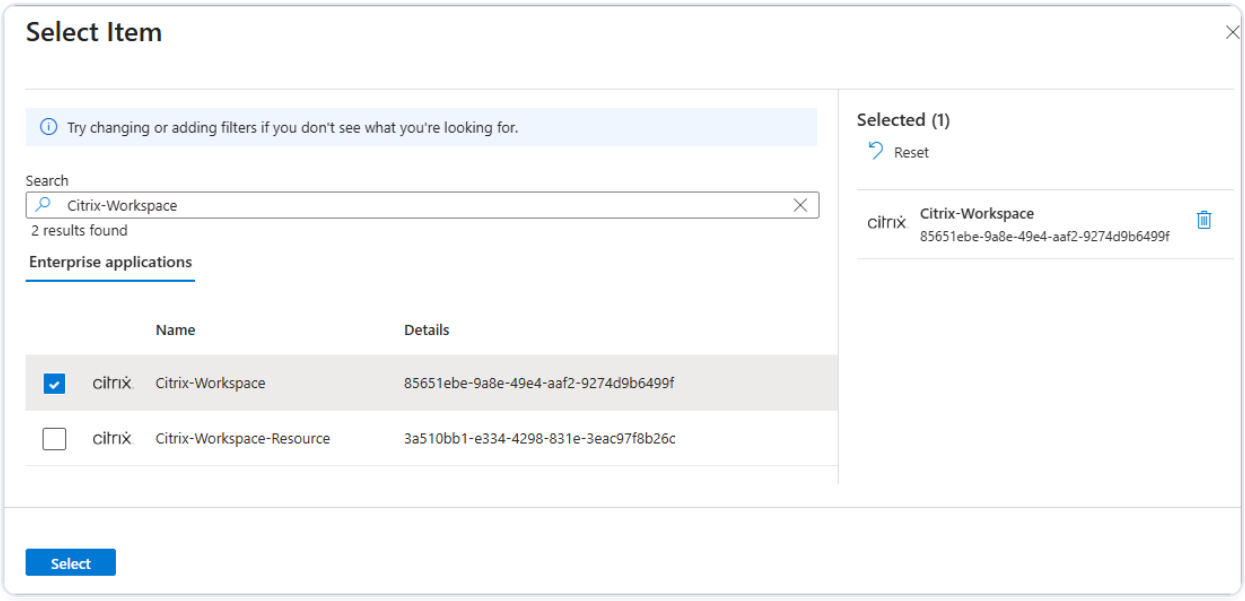
You must explicitly add the Citrix Client application as an approved client in the Citrix Resource application:

1. Click on the link to add your trusted client applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

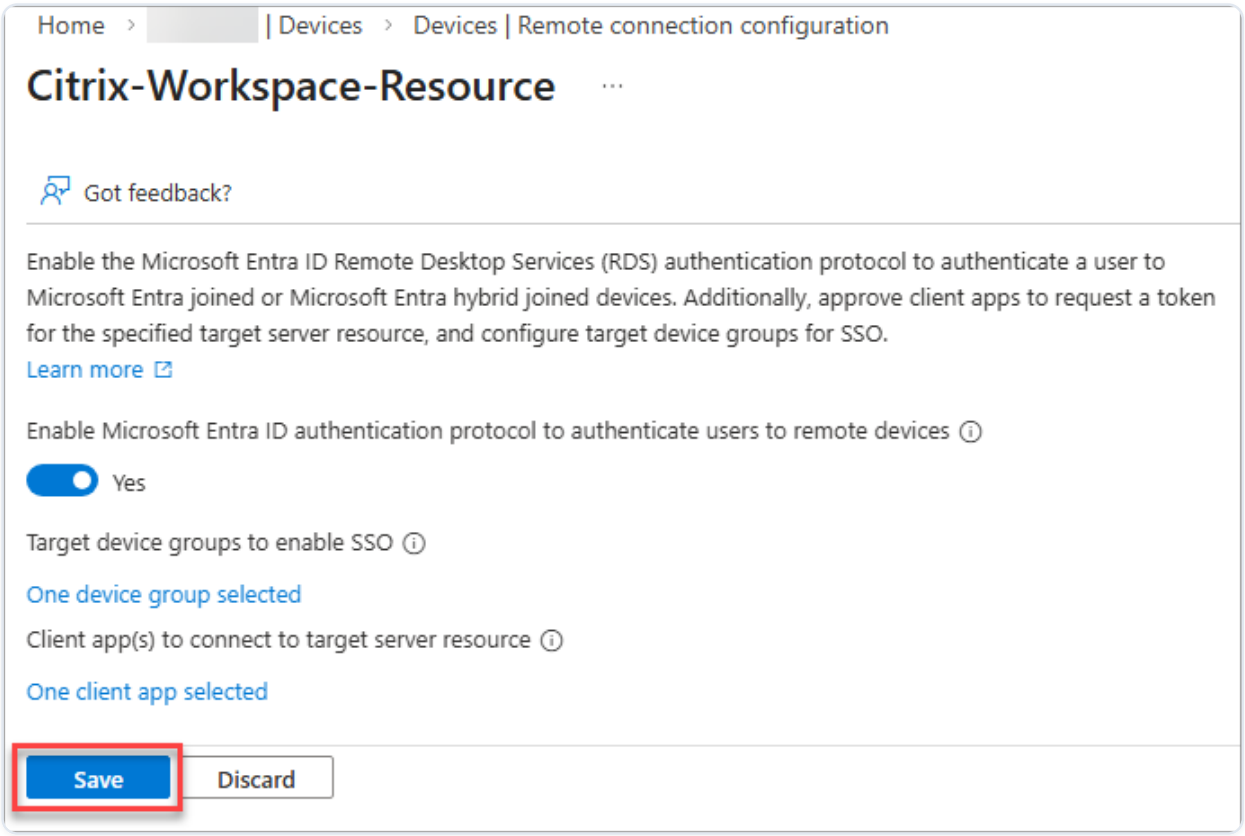


2. Select the Citrix Client application.



3. Select **Save** to apply the configuration changes to the Citrix Resource application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



CREATE A KERBEROS SERVER OBJECT

If your session hosts are Microsoft Entra hybrid joined, you must configure a Kerberos server object in the Active Directory domain where the user and computer accounts reside. See Create a Kerberos Server object for details.

REVIEW MICROSOFT ENTRA CONDITIONAL ACCESS POLICIES

If you use or plan to use Microsoft Entra Conditional Access policies, these need to be applied to the Citrix Resource application.

For detailed guidance on configuring Conditional Access when using Microsoft Entra single sign on for DaaS, refer to the Microsoft documentation. Remember that the required Conditional Access settings must be applied to the **Citrix Resource application**, not the Citrix Client application or Microsoft applications.

Citrix configuration

CITRIX SESSION HOSTS

Ensure the system requirements for the session hosts are met:

1. Ensure the session hosts are either Microsoft Entra joined or Microsoft Entra hybrid joined.
2. Install the required operating system version and build as specified in the system requirements.
3. Install the required VDA version as specified in the system requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Entra hybrid joined session hosts

If you are deploying Microsoft Entra hybrid joined session hosts with Citrix Machines Creation Services, Citrix Provisioning, or Windows 365, you can proceed to the next section. If you are provisioning Microsoft Entra hybrid joined hosts using any other tool or method, you must add the following registry value to your session hosts:

- Key: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
- Value type: **DWORD**
- Value name: `AzureADJoinType`
- Data: `1`

Session lock behavior

When a virtual desktop is locked, the default behavior is to display the Windows lock screen. At this point, the supported authentication methods for unlocking the desktop are **username and password** or **smart card**.

NOTE

Citrix web sign-in (preview) allows you to unlock your desktop using web-based Entra authentication. See Web sign-in for details.

If you have a passwordless deployment where users don't know their passwords, it's recommended to configure the session lock behavior to disconnect the session instead of showing the lock screen.

- **Multi-session session hosts**

  You can configure this behavior by enabling the **Disconnect remote session on lock for Microsoft identity platform authentication** setting through Intune or Group Policy. For detailed steps, see Configure the session lock behavior for Azure Virtual Desktop.

- **Single-session session hosts**

  If you are using **VDA version 2603 or newer**, you can configure this behavior by enabling the **Disconnect remote session on lock for Microsoft identity platform authentication** setting through Intune or Group Policy. For detailed steps, see Configure the session lock behavior for Azure Virtual Desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you are using VDA version 2511 or older, the **Disconnect remote session on lock for Microsoft identity platform authentication** setting is not supported. However, you can achieve the same behavior by creating a Windows scheduled task.

The following example script creates a scheduled task on single-session hosts that runs `cmd.exe /c tsdiscon` when the desktop is locked:

```
# Create the TaskService COM object

$service = New-Object -ComObject "Schedule.Service"

$service.Connect()



# Get the root folder and create a new task definition

$rootFolder = $service.GetFolder("\")

$taskDef = $service.NewTask(0)



# Registration info

$taskDef.RegistrationInfo.Description = "Disconnect session when
workstation is locked"



# Principal (Users group, least privilege)

$principal = $taskDef.Principal

$principal.GroupId = "S-1-5-32-545"

$principal.RunLevel = 0  # 0 = LeastPrivilege



# Settings

$settings = $taskDef.Settings
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$settings.Enabled = $true

$settings.AllowDemandStart = $true

$settings.DisallowStartIfOnBatteries = $false

$settings.StopIfGoingOnBatteries = $false

$settings.AllowHardTerminate = $false

$settings.StartWhenAvailable = $false

$settings.RunOnlyIfNetworkAvailable = $false

$settings.IdleSettings.StopOnIdleEnd = $true

$settings.IdleSettings.RestartOnIdle = $false

$settings.Hidden = $false

$settings.RunOnlyIfIdle = $false

$settings.DisallowStartOnRemoteAppSession = $false

$settings.UseUnifiedSchedulingEngine = $true

$settings.WakeToRun = $false

$settings.ExecutionTimeLimit = "PT0S"   # Unlimited

$settings.Priority = 7

$settings.MultipleInstances = 1         # IgnoreNew



# Trigger: SessionLock

$trigger = $taskDef.Triggers.Create(11)  # 11 =
TASK_TRIGGER_SESSION_STATE_CHANGE

$trigger.StateChange = 7                 # 7 = SessionLock
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$trigger.Enabled = $true



# Action: tsdiscon

$action = $taskDef.Actions.Create(0)     # 0 = Exec

$action.Path = "cmd.exe"

$action.Arguments = "/c tsdiscon"



# Register the task

$rootFolder.RegisterTaskDefinition(

    "Disconnect on Lock",  # Task name

    $taskDef,

    6,                     # TASK_CREATE_OR_UPDATE

    $null, $null,          # No specific user/password

    3                      # TASK_LOGON_GROUP

) | Out-Null
```

If you later need to remove the scheduled task, you can run the following command:

```
Unregister-ScheduledTask -TaskName "Disconnect on Lock" -Confirm:$false
```

CITRIX ACCESS AND CONTROL PLANE

Workspace authentication

You must configure Citrix® StoreFront Cloud to use Microsoft Entra ID or SAML as the IdP. Please refer to the Citrix® StoreFront Cloud documentation for details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If you are planning to use SAML as your IdP, you must ensure your SAML provider is configured properly to support Entra based authentication. See SAML using Microsoft Entra ID and Microsoft Entra identities for authentication.

Managing Workspace access

If your users will be accessing their store through a web browser, no additional configuration is required. If you want to enforce native access, you can configure Citrix® StoreFront Cloud to `Require end users to access their store from the Citrix client app` under the store's access configuration.

Enabling Microsoft Entra single sign-on in Workspace

After authentication is configured, you must enable the use of Microsoft Entra single sign-on:

1. Create a Service principal in Citrix Cloud:
    a. Go to **Identity and access management > API access > Service principals**.
    b. Click on **Create service principal**.
    c. Enter a **name** for the service principal and click **Next**.
    d. Set Access for the service principal:
        i. Select **Full access**, or
        ii. Select **Custom access > General > Citrix® StoreFront Cloud**, then click **Next**.
    e. Set the secret **expiration time** and click **Next**.
    f. Click **Complete**.
    g. Save both the secret and ID.
2. Download and extract the Citrix® StoreFront Cloud PowerShell module to your workstation, or any machine you can use for administrative purposes.
3. Open PowerShell in the machine in which you downloaded the Citrix® StoreFront Cloud PowerShell module.
4. Run the following commands:

```
Import-Module -Name
“<extractedPath>\Citrix.Workspace.StoreConfigs.psm1”

Set-StoreConfigurations -StoreUrl "https://
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<yourPrimaryStore>.cloud.com" -ClientId "<clientId>" -ClientSecret
"<clientSecret>" -AzureAdSsoEnabled $True
```

NOTE:

This is a global setting that will be applied to all the stores in your Citrix Cloud tenant. At this time, it is not possible to enable or disable this setting on specific stores based on the store URL provided in the command.

5. Run the following command to verify the setting was configured properly:

```
Get-StoreConfigurations -StoreUrl "https://
<yourPrimaryStore>.cloud.com" -ClientId "<clientId>" -ClientSecret
"<clientSecret>"
```

Delivery group configuration

1. If your session hosts are Microsoft Entra hybrid joined, assign the virtual apps and/or desktops to the appropriate Microsoft Entra users or groups. Any existing assignments to Active Directory users or groups may be removed, but it is not required.
2. If you are provisioning your Microsoft Entra joined session hosts with anything other than Citrix Machine Creation Services, Citrix Provisioning, or Windows 365, you will need to configure the logon type for the Delivery Groups. If you are using Microsoft Entra hybrid joined session hosts, the logon type for the delivery group must be configured regardless of provisioning method.

    a. If you do not already have the Citrix Remote PowerShell SDK installed, download it and install it on your workstation, or any machine you can use for administrative purposes.

    b. Open a PowerShell prompt in the machine in which you installed the Citrix Remote PowerShell SDK.

    c. Run the following commands:

    Microsoft Entra joined

    ```
    asnp citrix*

    Get-XDAuthentication
    ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-BrokerDesktopGroup -Name <dgName> | Set-BrokerDesktopGroup
-MachineLogOnType "AzureAd"
```

Microsoft Entra hybrid joined

```
asnp citrix*

Get-XDAuthentication

Get-BrokerDesktopGroup -Name <dgName> | Set-BrokerDesktopGroup
-MachineLogOnType "HybridAzureAd"
```

Configuring Microsoft Entra single sign-on on the VDA

By default, Microsoft Entra single sign-on is enabled on the VDA. To enable or disable this capability for a subset of session hosts, use the Microsoft Entra single sign-on policy setting.

CLIENT DEVICE

Ensure the system requirements for the client devices are met:

1. Install the required Citrix Workspace app version as specified in the system requirements.
2. If your users will be leveraging hybrid access, make sure the Citrix Web Extension is installed. If your users will be using native or browser access, the Citrix Web Extension is not needed.

Troubleshooting

Known issues

- After enabling Microsoft Entra single sign-on, users may encounter the Microsoft error **AADSTS293005** when launching their virtual desktop, indicating `RDP protocol is not enabled for the requested resource application. Please configure the RemoteDesktopSecurityConfiguration property on resource service principal to enable RDP protocol.` To resolve this issue, restart Citrix Workspace app.
- Users may encounter a 30-second delay when launching sessions if their Citrix Workspace app does not support Microsoft Entra single sign-on or if they use hybrid access without the Citrix Web Extension.
- Users may encounter a 30-second delay when launching sessions if Microsoft Entra single sign-on is enabled on Citrix® StoreFront Cloud and the required Azure configuration has not been completed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If the **Auto client reconnect authentication** setting is enabled, single sign-on will fail. As a workaround, disable this setting on the relevant session hosts.
- If **Keep me signed in (KMSI)** is disabled in Entra ID, single sign-on fails on Linux and macOS client devices.

When single sign-on fails

If single sign-on fails when accessing virtual desktops or applications, proceed as follows:

1. Confirm that Microsoft Entra single sign-on is enabled in Citrix® StoreFront Cloud.
2. Confirm that the access method leveraged by the user is supported.
3. If the user is leveraging hybrid access, confirm that the Citrix Web Extension is installed.
4. Confirm that the client device is running the required Citrix Workspace app version.
5. Confirm that your session hosts are running the required Windows build.
6. Confirm that your session hosts are running the required VDA version.
7. Ensure that the Windows setting `Always prompt for password upon connection` is not enabled on the session hosts.

   This setting is disabled by default, and can be configured through Group Policy or Intune under `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security`.

   You can check in the registry if the setting is enabled by looking for the value `fPromptForPassword` under `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services`. If the value is set to `1`, the setting is enabled and single sign-on will not be available. If the value is missing or set to `0`, the setting is disabled.
8. Ensure that the Windows setting `Allow Custom SSPs and APs to be loaded into LSASS` is enabled on the session hosts. This setting is enabled by default, and can be configured through Group Policy or Intune under `Computer Configuration\System\Local Security Authority`.
9. Confirm that the `AzureADJoinType` setting is configured correctly in the session hosts:
   - Key: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
   - Value type: **DWORD**
   - Value name: `AzureADJoinType`
   - Value data: `1` (Microsoft Entra hybrid joined); `2` (Microsoft Entra joined)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. Ensure that the virtual desktops or applications are assigned to Microsoft Entra identities instead of Active Directory identities in Citrix Studio.
11. Confirm that the Delivery Groups' logon type is configured correctly by running the following PowerShell command:

    ```
    Get-BrokerDesktopGroup -Name <deliveryGroupName>
    ```

    For Microsoft Entra joined session hosts, `MachineLogOnType` must be set to `AzureAd`. For Microsoft Entra hybrid joined session hosts, `MachineLogOnType` must be set to `HybridAzureAd`.
12. If you are using a SAML IdP, confirm that the necessary configuration was implemented.
13. Confirm that the Citrix Resource and Client applications are registered in the Microsoft Entra tenant.
14. Confirm that the Microsoft Entra ID RDS authentication protocol is enabled on the Citrix Resource application.
15. Confirm that the Citrix Client application was added as an approved client application in the Citrix Resource application.
16. If your session hosts are Microsoft Entra hybrid joined, confirm that a Kerberos server object was created in the Active Directory domain where the user and computer accounts reside.
17. Review your Microsoft Entra Conditional Access policies. Ensure no policies are being applied to the Citrix Client application and that any policies applied to the Citrix Resource application or the session hosts are configured properly so they don't affect the single sign-on experience.

Microsoft Entra single sign-on Azure configuration

In order to leverage Microsoft Entra single sign-on, you must first allow Microsoft Entra authentication for Windows in your Microsoft Entra ID tenant, which enables issuing the required authentication tokens that allow users to sign in to the Microsoft Entra joined and Microsoft Entra hybrid joined session hosts. To achieve this, you must do the following:

1. Register the Citrix applications (Resource app and Client app) in your Microsoft Entra ID tenant.
2. Enable the Remote Desktop Security Configuration for the Citrix resource application.
3. Add the Citrix client application as an approved client for the Citrix resource application.
4. \[Optional\] Hide the user consent prompt dialog.
5. Create a Kerberos server object.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Review Microsoft Entra Conditional Access policies.

The person making the Azure configuration must be assigned one of the following Microsoft Entra built-in roles or equivalent at a minimum:

- Application Administrator
- Cloud Application Administrator

If you wish to complete the Azure configuration via PowerShell, you will need to use the Microsoft Graph PowerShell SDK. You can also leverage Microsoft Graph API with a tool like Graph Explorer.

Instructions are provided for how to complete the configuration with both PowerShell and Graph Explorer.

PowerShell configuration

If you choose to use the Microsoft Graph PowerShell SDK, please note:

- You will need to use the Azure Cloud Shell with the PowerShell terminal type, or run PowerShell 7.x on your local system, and ensure your Azure context is set to the subscription that you want to use.
- You will need to install the Microsoft Graph PowerShell SDK v1.0 module (Microsoft.Graph) and the beta application module (Microsoft.Graph.Beta.Applications).

ENABLE REMOTE DESKTOP SECURITY CONFIGURATION

After you register the Citrix applications, you must enable the Remote Desktop Security Configuration in the Citrix Resource application.

1. Import the Authentication and Application Microsoft Graph modules and connect to Microsoft Graph with the `Application.Read.All` and `Application-RemoteDesktopConfig.ReadWrite.All` scopes:

```
Import-Module Microsoft.Graph.Authentication

Import-Module Microsoft.Graph.Applications

Import-Module Microsoft.Graph.Beta.Applications

Connect-MgGraph -Scopes "Application.Read.All","Application-
RemoteDesktopConfig.ReadWrite.All"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Get the object ID for the service principals associated with the app registrations:

   Citrix Cloud US, EU, APS

   ```
   $CtxResourceSpId = (Get-MgServicePrincipal -Filter "AppId eq '3a510bb1-
   e334-4298-831e-3eac97f8b26c'").Id

   $CtxClientSpId = (Get-MgServicePrincipal -Filter "AppId eq
   '85651ebe-9a8e-49e4-aaf2-9274d9b6499f'").Id
   ```

   Citrix Cloud Japan

   ```
   $CtxResourceSpId = (Get-MgServicePrincipal -Filter "AppId eq
   '0027603f-364b-40f2-98be-8ca4bb79bf8b'").Id

   $CtxClientSpId = (Get-MgServicePrincipal -Filter "AppId eq
   '0fa97bc0-059c-4c10-8c54-845a1fd5a916'").Id
   ```

3. Set the property `isRemoteDesktopProtocolEnabled` to `true`:

   ```
   If ((Get-MgServicePrincipalRemoteDesktopSecurityConfiguration
   -ServicePrincipalId $CtxResourceSpId) -ne $true) {

       Update-MgServicePrincipalRemoteDesktopSecurityConfiguration
   -ServicePrincipalId $CtxResourceSpId -IsRemoteDesktopProtocolEnabled

   }
   ```

4. Confirm the property `isRemoteDesktopProtocolEnabled` is set to `true`:

   ```
   Get-MgServicePrincipalRemoteDesktopSecurityConfiguration
   -ServicePrincipalId $CtxResourceSpId
   ```

APPROVE THE CLIENT APPLICATION

You must explicitly add the Citrix Client application as an approved client in the Citrix Resource application.

1. Create an `approvedClientApp` object:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$acp = New-Object -TypeName
Microsoft.Graph.Beta.PowerShell.Models.MicrosoftGraphApprovedClientApp

$acp.Id = $CtxClientSpId
```

2. Add the client app to the `approvedClientApp` object:

```
New-
MgBetaServicePrincipalRemoteDesktopSecurityConfigurationApprovedClientA
pp -ServicePrincipalId $CtxResourceSpId -BodyParameter $acp
```

The output should be similar to this:

```
Id                                   DisplayName

--                                   -----------

87654321-wxyz-1a2b-3c4d-1029384756af  Citrix-Workspace
```

HIDE THE USER CONSENT PROMPT DIALOG

By default, users are prompted to allow the Remote Desktop connection when connecting to a Microsoft Entra joined or Microsoft Entra hybrid joined session host with Microsoft Entra single sign-on enabled, in which they must select Yes to allow single sign-on. Microsoft Entra will remember up to 15 unique session hosts for 30 days before prompting again.

You can hide this dialog by configuring a list of target devices. To configure the list of devices, you must create one or more groups in Microsoft Entra ID that contain the Microsoft Entra joined and/or Microsoft Entra hybrid joined session hosts and then authorize the groups in the resource application, up to a maximum of 10 groups.

NOTE

It is highly recommended to create a dynamic group to simplify the membership management for the group. While dynamic groups normally update within 5-10 minutes, large tenants can take up to 24 hours.

Dynamic groups requires the Microsoft Entra ID P1 license or Intune for Education license. For more information, see Dynamic membership rules for groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Once the groups have been created, follow these steps:

1. Get the object ID (OID) of the group that contains the session hosts for which you want to hide the Remote Desktop connection prompt.
2. Create a `targetDeviceGroup` object:

```
$tdg = New-Object -TypeName
Microsoft.Graph.PowerShell.Models.MicrosoftGraphTargetDeviceGroup

$tdg.Id = "<groupOID>"
```

3. Add the client app to the `approvedClientApp` object:

```
New-
MgServicePrincipalRemoteDesktopSecurityConfigurationTargetDeviceGroup
-ServicePrincipalId $CtxResourceSpId -BodyParameter $tdg
```

   The output should be similar to this:

```
Id                                   DisplayName

--                                   -----------

87654321-wxyz-1a2b-3c4d-1029384756af  Entra-SSO-Desktops
```

4. If you later need to remove a device group from the targetDeviceGroup object, run the following command:

```
Remove-
MgServicePrincipalRemoteDesktopSecurityConfigurationTargetDeviceGroup
-ServicePrincipalId $CtxResourceSpId -TargetDeviceGroupId "<groupOID>"
```

NOTE

You can repeat these steps to add more groups if needed, up to a maximum of 10 groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Graph API configuration

ENABLE REMOTE DESKTOP SECURITY CONFIGURATION

After you register the Citrix applications, you must enable the Remote Desktop Security Configuration in the Citrix Resource application.

1. Get the object ID (OID) for the service principals associated with the app registrations from the Azure portal:
    a. Navigate to Microsoft Entra ID > Enterprise Applications.
    b. Remove the `Application type` filter if set so all applications are listed.
    c. Search for `Citrix-Workspace-Resource` / `Citrix-Workspace-Resource-JP` and note the associated object ID for the Resource application.
    d. Search for `Citrix-Workspace` / `Citrix-Workspace-JP` and note the associated object ID for the client application.
2. In Graph Explorer, sign in with an account from the target Azure tenant that has the required permissions.
3. Set the following query:
    - HTTP request method: PATCH
    - Microsoft Graph API Version: v1.0
    - Query:

    ```
    https://graph.microsoft.com/v1.0/servicePrincipals/<resourceAppOID>/
    remoteDesktopSecurityConfiguration
    ```

    - Request body:

    ```
    {

        "@odata.type":
    "#microsoft.graph.remoteDesktopSecurityConfiguration",

        "isRemoteDesktopProtocolEnabled": true

    }
    ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select the **Modify Permissions** tab and ensure that you have consented to the `Application.ReadWrite.All` permission.
5. Run the query.

See remoteDesktopSecurityConfiguration resource type for reference.

APPROVE THE CLIENT APPLICATION

You must explicitly add the Citrix Client application as an approved client in the Citrix Resource application.

Set the following query and run it:

- HTTP request method: POST
- Microsoft Graph API Version: v1.0
- Query:

```
https://graph.microsoft.com/v1.0/servicePrincipals/<resourceAppOID>/
remoteDesktopSecurityConfiguration/approvedClientApps
```

- Request body:

```
{

    "@odata.type": "#microsoft.graph.approvedClientApp",

    "id": "<clientAppOID>"

}
```

HIDE THE USER CONSENT PROMPT DIALOG

By default, users are prompted to allow the Remote Desktop connection when connecting to a Microsoft Entra joined or Microsoft Entra hybrid joined session host with Microsoft Entra single sign-on enabled, in which they must select Yes to allow single sign-on. Microsoft Entra will remember up to 15 unique session hosts for 30 days before prompting again.

You can hide this dialog by configuring a list of target devices. To configure the list of devices, you must create one or more groups in Microsoft Entra ID that contain the Microsoft Entra joined and/or Microsoft Entra hybrid joined session hosts and then authorize the groups in the resource application, up to a maximum of 10 groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

It is highly recommended to create a dynamic group to simplify the membership management for the group. While dynamic groups normally update within 5-10 minutes, large tenants can take up to 24 hours.

Dynamic groups requires the Microsoft Entra ID P1 license or Intune for Education license. For more information, see Dynamic membership rules for groups.
Once the groups have been created, follow these steps:

1. Get the object ID (OID) of the group that contains the session hosts for which you want to hide the Remote Desktop connection prompt.
2. Set the following query and run it:
   - HTTP request method: POST
   - Microsoft Graph API Version: v1.0
   - Query:

     ```
     https://graph.microsoft.com/v1.0/servicePrincipals/<resourceAppOID>/
     remoteDesktopSecurityConfiguration/targetDeviceGroups
     ```

   - Request body:

     ```
     {

         "@odata.type": "#microsoft.graph.targetDeviceGroup",

         "id": "<groupOID>"

     }
     ```

NOTE

You can repeat these steps to add more groups if needed, up to a maximum of 10 groups.

If you later need to remove a device group from the targetDeviceGroup object, set the following and run the query:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HTTP request method: DELETE
- Microsoft Graph API Version: v1.0
- Query:

```
https://graph.microsoft.com/beta/servicePrincipals/<resourceAppOID>/
remoteDesktopSecurityConfiguration/targetDeviceGroups
```

See targetDeviceGroup resource type for reference.

CREATE A KERBEROS SERVER OBJECT

If your session hosts are Microsoft Entra hybrid joined, you must configure a Kerberos server object in the Active Directory domain where the user and computer accounts reside. See Create a Kerberos Server object for details.

REVIEW MICROSOFT ENTRA CONDITIONAL ACCESS POLICIES

If you use or plan to use Microsoft Entra Conditional Access policies, review the configuration applied to the **Citrix Resource application** and the **Citrix Client application** to ensure users have the intended sign-in experience.

For detailed guidance on configuring Conditional Access when using Microsoft Entra single sign-on for DaaS, refer to the Microsoft documentation. Remember that the required Conditional Access settings must be applied to the **Citrix Resource application** or **Citrix Client application**, not the Microsoft applications.

Federated Authentication Service

Citrix Federated Authentication Service (FAS) enables single sign-on (SSO) to Citrix virtual desktops and applications in environments where users authenticate through modern identity providers such as SAML or OpenID Connect (OIDC) that don’t supply a Windows password, ensuring seamless access to session hosts joined to an Active Directory domain.

See the Federated Authentication Service documentation for more details.

Smart cards

Citrix Virtual Apps and Desktops and Citrix DaaS support smart cards both for logging into virtual desktops and applications and for use within active sessions. Smart cards provide certificate-based, two-factor authentication that strengthens security by requiring both the physical card and a PIN. This allows organizations to meet compliance requirements, protect sensitive data, and streamline access for users who already rely on smart cards for Windows logon or secure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

applications. Once authenticated, users can also use their smart cards inside the session to digitally sign documents, encrypt email, or access other smart card–enabled applications, ensuring a consistent and secure experience across both local and virtual environments.

See the smart cards documentation for more details.

Web sign-in

You can use the Citrix web sign-in credential provider to enable the use of Entra ID based Windows authentication. This allows users to log into or unlock their virtual desktops using any authentication method that is enabled in Entra ID.

IMPORTANT

Web sign-in is currently in preview. This feature is provided without support and is not yet recommended for use in production environments.

System requirements

The following are the system requirements for using web sign-in:

- Virtual Delivery Agent
  - Windows: **single session** version 2607 or later
- Citrix Workspace app
  - Windows: version 2607 or later
- Session host identity: Entra joined or Entra hybrid joined
- Session host OS:
  - Windows 11, version 24H2 with 2025-09 Cumulative Updates for Windows 11 (KB5065789) or later installed (build 26100.6725)

How to configure web sign-in

Citrix web sign-in is disabled by default. To enable it, follow these steps:

1. Complete the **Azure and Microsoft Entra ID configuration** described in the Microsoft Entra single sign-on documentation. If you have Microsoft Entra single sign-on enabled in your environment, you can continue to the next step.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The relevant steps are:

a. Register the Citrix resource and client applications.
b. Enable the Microsoft Entra ID Remote Desktop Services authentication protocol for the Citrix resource application.
c. Hide the user consent prompt.
d. Approve the client application.
e. Create a Kerberos server object (Microsoft Entra hybrid joined environments only).
f. Review Microsoft Entra Conditional Access policies.

2. Enable the **Web sign-in** setting in a Citrix policy and apply the policy to the appropriate delivery groups.

NOTE

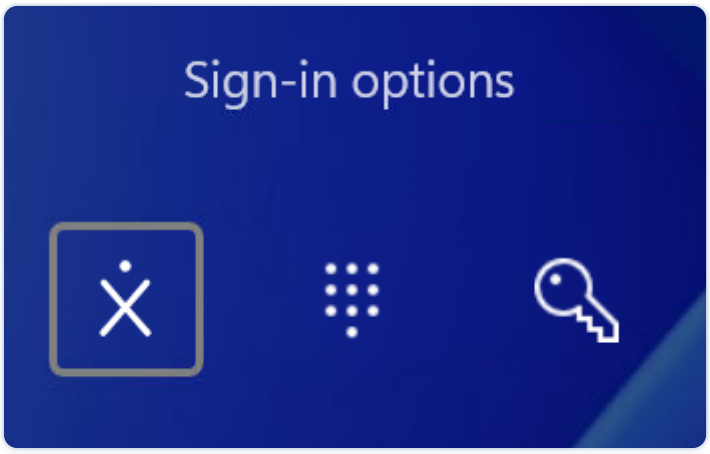
- It is not necessary to use Microsoft Entra single sign-on to use web sign-in.
- If the policy setting is not yet available in your tenant, you can enable web sign-in via the registry:
  - Key: HKLM\SOFTWARE\Policies\Citrix\ICAPolicies
  - Value type: DWORD
  - Value name: AllowWebSignIn
  - Value data: 1

How to use web sign-in

To use Citrix web sign-in to log in or unlock your virtual desktop:

1. Select the Citrix tile from the logon methods available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Click on **Citrix Web Sign-in**.



3. Once the authentication prompt pops up, authenticate with the required authentication method.

NOTE

The authentication methods available to the user are determined by what is enabled in Microsoft Entra ID.

Set up resource locations

Resource locations contain the resources required to deliver applications and desktops to users. You manage the resources from Citrix Cloud. Typically, resources include:

- Hypervisors or cloud services, known as *hosts* that include:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Active Directory domain controllers.
- Virtual Delivery Agents (VDAs): VDAs are installed on a machine that delivers the applications and desktops to the users.
- Citrix Gateway (optional): To enable secure external access to the applications and desktops offered to users, add a Citrix Gateway VPX appliance to the resource location. Then, set up Citrix Gateway.
- Citrix StoreFront™ servers.
- To communicate with Citrix Cloud, every resource location must contain a Citrix Cloud Connector. A minimum of two Cloud Connectors per resource location is recommended.

A zone is equivalent to a resource location. When you create a resource location and install a Cloud Connector, a zone is automatically created for you. For more information, see Zones.

To learn more about resource types, see Connect to Citrix Cloud.

Host requirements

The hypervisor or cloud service, where you provision VMs, need unique permissions or setup.

- If the hypervisor or cloud service requires virtual networks, follow the guidance in its documentation.
- Create the appropriate Virtual Private Cloud (VPC) (for AWS or GCP) or Virtual Network (VNET) (for Azure) for the machines that you'll add to your resource location.
- Create the appropriate rules to secure inbound and outbound traffic between machines in the virtual network. For example, when using AWS, ensure that the VPC's security group has the appropriate rules configured so that machines in the VPC are accessible to only the IP addresses you specify.

The following host types are supported:

- Amazon Web Services (AWS) virtualization environments
- XenServer® virtualization environments
- Google Cloud Platform virtualization environments
- HPE Moonshot virtualization environments
- Microsoft Azure Resource Manager virtualization environments
- Microsoft System Center Virtual Machine Manager virtualization environments
- Nutanix virtualization environments

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Nutanix cloud and partner solutions
- VMware virtualization environments
- VMware cloud and partner solutions

Active Directory

Provision a Windows server, install Active Directory Domain Services (AD DS), and promote it to a Domain Controller. For guidance, see the Microsoft documentation on Active Directory Domain Services Overview.

The important considerations are:

- You must have at least one Domain Controller running Active Directory Domain Services.
- Do not install any Citrix components on a Domain Controller.

For more information, see:

- Active Directory functional levels
- Identity and access management in Citrix Cloud.
- Connect Active Directory to Citrix Cloud
- Deployment scenarios for using Connector Appliance with Active Directory

Cloud Connectors

The Cloud Connector is a group of services from Citrix Cloud that allow communication between the VDAs, StoreFront, and the cloud-based Delivery Controller. You can install Cloud Connectors interactively or from the command line.

For more information on Cloud Connectors, see:

- Citrix Cloud Connector
- Technical details
- Proxy and firewall configuration
- Installation
- Connector updates

Size and scale considerations

- When evaluating Citrix DaaS™ for sizing and scalability, consider all components.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Research and test the configuration of the Cloud Connectors and StoreFront for your specific requirements.
- Undersizing the machines can impact system performance negatively.

The article Size and scale considerations for Cloud Connectors includes:

- Size and scale testing information
- Tested maximum capacities
- Best practice recommendations for Cloud Connector machine configuration

Add a resource type

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **Resource Locations**.
3. Select **+ Resource Locations** to add a resource location.
4. Enter a name for the resource location, and then click **Save**. For information about naming considerations, see Name restrictions.
5. Under the new resource location, select **+ Cloud Connectors**.
6. Download and install the Cloud Connector software on at least two servers in the domain where you have your Citrix DaaS resources.
   - During the installation, select the resource location you created in the previous steps.
   - After installation, Citrix Cloud adds the servers to the resource location, and registers the domains in which you installed the Cloud Connectors.
7. Verify that the registered domains are active:
   - From the Citrix Cloud menu, select **Identity Access Management**.
   - Select **Domains**. A list of domains where Cloud Connectors have been deployed displays.
   - Locate the domains that you are using with Citrix DaaS. Active domains display with a green bar on the left side of the domain entry.

   If your domain does not have the visual indicator, the domain is in an **unused** state. If you specify an unused domain during machine catalog setup, catalog creation fails. To ensure machine catalog setup occurs without errors, follow the steps in Activate an unused domain.

   For more information, see CTX473009: DaaS Catalog Creation Wizard: "Internal Server Error" when creating adding new machine accounts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Activate an unused domain

1. From the **Domain** tab, in **Identity and Access Management**, select **Show Unused Domains**. After you select this option, the label changes to **Hide Unused Domains**.
2. Locate the unused domain in the list. Unused domains display a gray bar on the left side of the domain entry, and a single-option ellipsis menu on the right side.
3. Select the ellipsis menu, and then select **Use domain**. The gray bar becomes green, and the ellipsis menu change to **Disable**.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For setting up resource location for specific host types:
  - AWS virtualization environments
  - Google Cloud virtualization environments
  - HPE Moonshot virtualization environments
  - Microsoft Azure Resource Manager virtualization environments
  - Microsoft System Center Virtual Machine Manager virtualization environments
  - Nutanix virtualization environments
  - Nutanix cloud and partner solutions
  - VMware virtualization environments
  - VMware cloud and partner solutions
  - XenServer virtualization environments
- For a full deployment, Create and manage connections and resources to a resource location.
- Review all the steps in the installation and configuration process

Amulet Hotkey CoreStation virtualization environments

Citrix DaaS™ manages your Amulet Hotkey CoreStation workloads through a Citrix-managed Amulet Hotkey CoreStation plug-in present in the DaaS control plane. With this plug-in, you can create connections to your Amulet Hotkey CoreStation enclosure, create catalogs, and power manage machines in the catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Key steps

1. Set up your Amulet Hotkey CoreStation environment.
2. Create a connection to the Amulet Hotkey CoreStation enclosure.
3. Create a machine catalog.

   NOTE:

   Before creating a catalog, ensure to have one or more Amulet Hotkey CoreStation nodes and install VDAs on those nodes. You can consider the Amulet Hotkey CoreStation enclosure as the hypervisor and the nodes as VMs.

4. Create a delivery group.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine that will deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to Amulet Hotkey CoreStation.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

AWS virtualization environments

This article describes how to set up your AWS account as a resource location you can use with Citrix DaaS. The resource location is used for provisioning workloads in AWS EC2 and Amazon WorkSpaces Core Managed Instances. For the list of OS types supported for Amazon WorkSpace Core Managed Instances, see VDAs in Amazon WorkSpaces Core Managed Instances.

Comparison of different configurable resource locations: MCS for AWS EC2, MCS for Amazon WorkSpaces Core Managed Instances, and Quick Deploy for Amazon WorkSpaces Core Bundles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MCS FOR AWS EC2	MCS FOR AMAZON WORKSPACES CORE MANAGED INSTANCES	QUICK DEPLOY FOR AMAZON WORKSPACES CORE BUNDLES
Citrix® handles provisioning of VMs in your AWS account	Citrix handles provisioning of VMs in your AWS account	Amazon handles provisioning of VMs in AWS-managed WorkSpaces account
Advanced MCS workflow for VM lifecycle management	Advanced MCS workflow for VM lifecycle management	5-step quick and easy workflow
EC2 instances	WorkSpaces Core Managed Instances (utilize on-demand EC2 instances launched directly into your AWS account)	WorkSpaces Bundles, fully AWS-managed capacity (higher level abstraction)
No Microsoft 365 licensing support	BYOL Microsoft 365 support	BYOL Microsoft 365 support
Windows Server, Windows Desktop, and Linux	Windows Server, Windows Desktop, and Linux	Windows Server, Windows Desktop
Persistent and Non-persistent VMs	Persistent and Non-persistent VMs	Persistent VMs only
Pay-as-you-go only	Pay-as-you-go	Fixed price per month only
Citrix DaaS and Citrix Virtual Apps and Desktops™	Citrix DaaS and Citrix Virtual Apps and Desktops™	Citrix DaaS only

The resource location includes a basic set of components, ideal for a proof-of-concept, or other deployment that does not require resources spread over multiple availability zones.

When you complete the tasks in this article, your resource location includes the following components:

- A virtual private cloud (VPC) with public and private subnets inside a single availability zone.
- An instance that runs as both an Active Directory Domain Controller and DNS server, located in the private subnet of the VPC.
- Two domain-joined instances on which the Citrix Cloud Connector™ is installed, located in the private subnet of the VPC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- An instance that acts as a bastion host, located in the public subnet of your VPC. This instance is used to initiate RDP connections to the instances in the private subnet for administration purposes. After you finish setting up your resource location, you can shut down this instance so it is no longer readily accessible. When you must manage other instances in the private subnet, such as VDA instances, you can restart the bastion host instance.

After you complete the tasks, you can install VDAs, provision machines, create machine catalogs, and create Delivery Groups.

Task overview

Set up a virtual private cloud (VPC) with public and private subnets. When you complete this task, AWS deploys NAT gateways with an Elastic IP address in the public subnet. This enables instances in the private subnet to access the Internet. Instances in the public subnet are accessible to inbound public traffic while instances in the private subnet are not.

Configure security groups. Security groups act as virtual firewalls that control traffic for the instances in your VPC. You add rules to your security groups that allow instances in your public subnet to communicate with instances in your private subnet. You also associate these security groups with each instance in your VPC.

Create a DHCP options set. An Amazon VPC, DHCP, and DNS services are provided by default, which affects how you configure DNS on your Active Directory Domain Controller. Amazon's DHCP cannot be disabled and Amazon's DNS can be used only for public DNS resolution, not Active Directory name resolution. To specify the domain and name servers handed to instances through DHCP, create a DHCP options set. The set assigns the Active Directory domain suffix and specifies the DNS server for all instances in your VPC. To ensure Host (A) and Reverse Lookup (PTR) records are automatically registered when instances join the domain, you configure the network adapter properties for each instance you add to the private subnet.

Add a bastion host, Domain Controller, and Cloud Connectors to the VPC. Through the bastion host, you can log on to instances in the private subnet to set up the domain, join instances to the domain, and install the Cloud Connector.

Task 1: Set up the VPC

1. From the AWS management console, select **VPC**.
2. From the VPC Dashboard, select **Create VPC**.
3. Select **VPC and more**.
4. Under NAT gateways ($), select **In 1 AZ** or **1 per AZ**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Under DNS options, leave **Enable DNS hostnames** selected.
6. Select **Create VPC**. AWS creates the public and private subnets, Internet gateway, route tables, and default security group.

NOTE:

Changing the name of an AWS Virtual Private Cloud (VPC) in the AWS console breaks the existing hosting unit in the Citrix Cloud. When the hosting unit is broken, you cannot create catalogs or add machines to existing catalogs. From Known Issue: PMCS-7701

Task 2: Configure security groups

This task creates and configures the following security groups for your VPC:

- A public security group to associate with the instances in your Public subnet.
- A private security group to associate with the instances in your Private subnet.

To create the security groups:

1. In the VPC Dashboard, select **Security Groups**.
2. Create a security group for the public security group. Select **Create Security Group** and enter a name tag and description for the group. In VPC, select the VPC you created earlier. Select **Yes, Create**.

Configure the Public security group

1. From the security group list, select the Public security group.
2. Select the **Inbound Rules** tab and select Edit to create the following rules:

TYPE	SOURCE
ALL Traffic	Select the Private security group.
ALL Traffic	Select the Public security group.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE	SOURCE
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Session Reliability)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. When finished, select **Save**.
4. Select the **Outbound Rules** tab and select **Edit** to create the following rules.

TYPE	DESTINATION
ALL Traffic	0.0.0.0/0

5. When finished, select **Save**.

Configure the private security group

1. From the security group list, select the Private security group.
2. If you have not yet setup traffic from the public security group, you must set TCP ports. Select the **Inbound Rules** tab and select **Edit** to create the following rules:

TYPE	SOURCE
ICMP	Select the Public security group.
TCP 53 (DNS)	Select the Public security group.
UDP 53 (DNS)	Select the Public security group.
80 (HTTP)	Select the Public security group.
TCP 135	Select the Public security group.
TCP 389	Select the Public security group.
UDP 389	Select the Public security group.
443 (HTTPS)	Select the Public security group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE	SOURCE
TCP 1494 (ICA/HDX)	Select the Public security group.
TCP 2598 (Session Reliability)	Select the Public security group.
3389 (RDP)	Select the Public security group.
TCP 49152–65535	Select the Public security group.

3. When finished, select **Save.**
4. Select the **Outbound Rules** tab and select **Edit** to create the following rules.

TYPE	DESTINATION
ALL Traffic	Select the Private security group.
ALL Traffic	0.0.0.0/0

5. When finished, select **Save**.

Task 3: Launch instances

Do the following steps to create four EC2 instances and decrypt the default Administrator password that Amazon generates:

1. From the AWS management console, select **EC2**.
2. From the EC2 Dashboard, select **Launch Instance**.
3. Select a Windows Server machine image and instance type.
4. On the **Configure Instance Details** page, enter a name for the instance and select the VPC that you had set up earlier.
5. In **Subnet**, make the following selections for each instance:
    - Bastion host: Select the Public subnet
    - Domain controller and Connectors: Select the Private subnet
6. In **Auto-assign Public IP address**, make the following selections for each instance:
    - Bastion host: Select **Enable**
    - Domain controller and Connectors: Select **Use default setting** or **Disable**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. In **Network Interfaces**, enter a primary IP address within the IP range of your private subnet for the Domain Controller and Cloud Connector instances.
8. If necessary, on the **Add Storage** page, modify the disk size.
9. On the **Tag Instance** page, enter a friendly name for each instance.
10. On the **Configure Security Groups** page, select **Select an existing security group** and then make the following selections for each instance:
    - Bastion host: Select the Public security group.
    - Domain controller and Cloud Connectors: Select the Private security group.
11. Review your selections and then select **Launch**.
12. Create a new key pair or select an existing one. If you create a new key pair, then download your private key (`.pem`) file and keep it in a safe place. You must supply your private key when you acquire the default Administrator password for the instance.
13. Select **Launch Instances**. Select **View Instances** to display a list of your instances. Wait until the newly launched instance has passed all status checks before accessing it.
14. Acquire the default Administrator password for each instance.
    a. From the instance list, select the instance and then select **Connect**.
    b. Go to the **RDP client** tab, select **Get Password**, and upload your private key (`.pem`) file when prompted.
    c. Select **Decrypt Password** to get the human readable password. AWS displays the default password.
15. Repeat all the steps from step 2 until you have created four instances:
    - One bastion host instance in your public subnet
    - Three instances in your private subnet to be used as:
        - One as a Domain Controller
        - Two as Cloud Connectors

Task 4: Create a DHCP options set

1. From the VPC Dashboard, select **DHCP Options Sets**.
2. Enter the following information:
    - Name tag: Enter a friendly name for the set.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Domain name: Enter the fully qualified domain name that you use when you configure the Domain Controller instance.
- Domain name servers: Enter the private IP address you assigned to the Domain Controller instance and the string **AmazonProvidedDNS**, separated by commas.
- NTP servers: Leave this field blank.
- NetBIOS name servers: Enter the private IP address of the Domain Controller instance.
- NetBIOS node type: Enter **2**.

3. Select **Yes, Create.**
4. Associate the new set with your VPC:

   a. From the VPC Dashboard, select **Your VPCs** and then select the VPC you set up earlier.

   b. Select **Actions > Edit DHCP Options Set**.

   c. When prompted, select the new set you created, and then select **Save**.

Task 5: Configure the instances

1. Using an RDP client, connect to the public IP address of the bastion host instance. When prompted, enter the credentials for the Administrator account.
2. From the bastion host instance, launch **Remote Desktop Connection** and connect to the private IP address of the instance you want to configure. When prompted, enter the Administrator credentials for the instance.
3. For all instances in the private subnet, configure the DNS settings:

   a. Select **Start > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**. Double-click the network connection displayed.

   b. Select **Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties**.

   c. Select **Advanced > DNS**. Ensure that the following settings are enabled, and then select **OK**:

      - **Register this connection's addresses in DNS**
      - **Use this connection's DNS suffix in DNS registration**

4. Configure the Domain Controller:

   a. Using Server Manager, add the Active Directory Domain Services role with all default features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Promote the instance to a Domain Controller. During promotion, enable DNS and use the domain name you specified when you created the DHCP options set. Restart the instance when prompted.

5. Configure the first Cloud Connector:

   a. Join the instance to the domain and restart when prompted. From the bastion host instance, reconnect to the instance using RDP.

   b. Sign in to Citrix Cloud. Select **Resource Locations** from the upper left menu.

   c. Download the Cloud Connector.

   d. When prompted, run the `cwcconnector.exe` file and supply your Citrix Cloud credentials. Follow the wizard.

   e. Once complete, select **Refresh** to display the **Resource Locations** page. When the Cloud Connector is registered, the instance appears on the page.

6. Repeat the steps to configure the Cloud Connector to configure the second Cloud Connector.

7. Attach an IAM Policy to the Cloud Connectors to support AWS hosting connections with role-based authorization. You must have the same IAM Policy attached to all the Cloud Connectors in a resource location. For information about AWS permissions, see Required AWS permissions-Amazon EC2 and Required AWS permissions-Amazon WorkSpaces Core Managed Instances.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see:
  - Connection to AWS
  - Connection to Amazon WorkSpaces Core Managed Instances
- Review all the steps in the installation and configuration process

More information

- Create and manage connections and resources
- Create machine catalogs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Google Cloud virtualization environments

Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) lets you provision and manage machines on Google Cloud.

Prerequisites

Before you start provisioning the VMs to Google Cloud Platform (GCP), you must make sure the following prerequisites are met.

1. The Citrix subscription must include support for Hybrid Multi-Cloud workloads. For more information, see Compare Citrix subscription features.
2. The admin account must have sufficient permissions to create host connections, machine catalogs, and delivery groups. For more information, see Configure Delegated Administration.
3. Identify a Google Cloud project, in which all compute resources associated with the machine catalog are stored. It can be an existing project or a new one. For more information, see Google Cloud projects.
4. Enable the Google Cloud APIs required for the integration with Citrix DaaS. For more information, see Enable Google Cloud APIs.
5. Create the service accounts in Google Cloud and grant the appropriate permissions. For more information, see Configure and update service accounts.
6. Download the key file for the Citrix Cloud Service Account. For more information, see Citrix Cloud Service Account key.
7. The virtual machines must have access to the Google APIs without a public IP address. For more information, see Enable Private Google Access.

Google Cloud projects

There are basically two types of Google Cloud projects:

- Provisioning project: In this case, the current admin account owns the provisioned machines in the project. This project is also referred to as a local project.
- Shared VPC project: Project in which machines created in the provisioning project use the VPC from the Shared VPC project. The admin account used for provisioning projects has limited permissions in this project, specifically, only permissions to use the VPC.

Service endpoint URLs

You must have access to the following URLs:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Enable Google Cloud APIs

To use the Google Cloud functionality through Studio, enable these APIs in your Google Cloud project:

- Compute Engine API
- Cloud Resource Manager API
- Identity and Access Management (IAM) API
- Cloud Build API

From the Google Cloud console, complete these steps:

1. In the upper left menu, select **APIs and Services > Enabled APIs & services**.
2. On the **Enabled APIs & services** screen, ensure that the Compute Engine API is enabled. If not, follow these steps:
    a. Navigate to **APIs and Services > Library**.
    b. In the search box, type *Compute Engine*.
    c. From the search results, select **Compute Engine API**.
    d. On the **Compute Engine API** page, select **Enable**.
3. Enable Cloud Resource Manager API.
    a. Navigate to **APIs and Services > Library**.
    b. In the search box, type *Cloud Resource Manager*.
    c. From the search results, select **Cloud Resource Manager API**.
    d. On the **Cloud Resource Manager API** page, select **Enable**. The status of the API appears.
4. Similarly, enable **Identity and Access Management (IAM) API** and **Cloud Build API**, and **Cloud Key Management Service (KMS) API**.

You can also use Google Cloud Shell to enable the APIs. To do this:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the Google Console and load the Cloud Shell.
2. Run the following four commands in the Cloud Shell:
   - gcloud services enable compute.googleapis.com
   - gcloud services enable cloudresourcemanager.googleapis.com
   - gcloud services enable iam.googleapis.com
   - gcloud services enable cloudbuild.googleapis.com
   - gcloud services enable cloudkms.googleapis.com
3. Click **Authorize** when the Cloud Shell prompts.

Configure and update service accounts

NOTE:

GCP is introducing changes to Cloud Build Service's default behavior and use of service accounts after April 29, 2024. For more information, see Cloud Build Service Account Change. Your existing Google projects with Cloud Build API enabled before April 29, 2024 are not affected by this change. However, if you want to have existing Cloud Build Service behavior after April 29, you can create or apply the organization policy to disable the constraint enforcement before you enable the Cloud Build API. As a result, the following content is divided into two: Before April 29, 2024 and After April 29, 2024. If you set the new organization policy, follow the section Before April 29, 2024.

Before April 29, 2024

Citrix Cloud™ uses three separate service accounts within the Google Cloud project:

- *Citrix Cloud Service Account*: This service account enables Citrix Cloud to access the Google project, provision, and manage machines. This service account authenticates to Google Cloud using a key generated by Google Cloud.

  You must create this service account manually as outlined here. For more information, see Create a Citrix Cloud Service Account.

  You can identify this service account with an email address. For example, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Cloud Build Service Account*: This service account is provisioned automatically after you enable all the APIs mentioned in Enable Google Cloud APIs. To view all automatically created service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

accounts, navigate to **IAM & Admin > IAM** in the **Google Cloud** console and select the **Include Google-provided role grants** checkbox.

You can identify this service account by an email address that begins with the **Project ID** and the word **cloudbuild**. For example, `<project-id>@cloudbuild.gserviceaccount.com`

Verify if the service account has been granted the following roles. If you must add roles, follow the steps outlined in Add roles to the Cloud Build Service Account.

- Cloud Build Service Account
- Compute Instance Admin
- Service Account User

- *Cloud Compute Service Account*: This service account is added by Google Cloud to instances created in Google Cloud once the Compute API is activated. This account has the IAM basic editor role to do the operations. However, if you delete the default permission to have more granular control, you must add a **Storage Admin** role that requires the following permissions:
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

You can identify this service account by an email address that begins with the **Project ID** and the word **compute**. For example, `<project-id>-compute@developer.gserviceaccount.com`.

CREATE A CITRIX CLOUD SERVICE ACCOUNT

To create a Citrix Cloud Service Account, follow these steps:

1. In the Google Cloud console, navigate to **IAM & Admin > Service accounts**.
2. On the **Service accounts** page, select **CREATE SERVICE ACCOUNT**.
3. On the **Create service account** page, enter the required information, and then select **CREATE AND CONTINUE**.
4. On the **Grant this service account access to project** page, click the **Select a role** drop-down menu and select the required roles. Click **+ADD ANOTHER ROLE** if you want to add more roles.

   Each account (personal or service) has various roles defining the management of the project. Grant the following roles to this service account:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Compute Admin
- Storage Admin
- Cloud Build Editor
- Service Account User
- Cloud Datastore User
- Cloud KMS Crypto Operator

The Cloud KMS Crypto Operator requires the following permissions:

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

NOTE:

Enable all the APIs to get the complete list of roles available while creating a new service account.

5. Click **CONTINUE**
6. On the **Grant users access to this service account** page, add users or groups to grant them access to perform actions in this service account.
7. Click **DONE**.
8. Navigate to the IAM main console.
9. Identify the service account created.
10. Validate the roles are assigned successfully.

Considerations:

When creating the service account, consider the following:

- The steps **Grant this service account access to project** and **Grant users access to this service account** are optional. If you choose to skip these optional configuration steps, the newly created service account does not display in the **IAM & Admin > IAM** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To display roles associated with a service account, add the roles without skipping the optional steps. This process ensures that roles appear for the configured service account.

CITRIX CLOUD SERVICE ACCOUNT KEY

The Citrix Cloud Service Account key is required for creating a connection in Citrix DaaS. The key is contained in a credential file (.json). The file is automatically downloaded and saved to the **Downloads** folder after you create the key. When you create the key, be sure to set the key type to JSON. Otherwise, Studio cannot parse it.

To create a Service Account Key, navigate to **IAM & Admin > Service accounts** and click the email address of the Citrix Cloud Service Account. Switch to the **Keys** tab and select **Add Key > Create new key**. Make sure to select **JSON** as the key type.

TIP:

Create keys using the **Service accounts** page in the Google Cloud console. We recommend that you change keys regularly for security purposes. You can provide new keys to the Citrix Virtual Apps and Desktops application by editing an existing Google Cloud connection.

ADD ROLES TO THE CITRIX CLOUD SERVICE ACCOUNT

To add roles to the Citrix Cloud Service Account:

1. In the Google Cloud console, navigate to **IAM & Admin > IAM**.
2. On the **IAM > PERMISSIONS** page, locate the service account you created, identifiable with an email address.

   For example, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Select the pencil icon to edit the access to the principal of the service account.
4. On the **Edit access to "project-id"** page for the selected principal option, select **ADD ANOTHER ROLE** to add the required roles to your service account one by one and then select **SAVE**.

ADD ROLES TO THE CLOUD BUILD SERVICE ACCOUNT

To add roles to the Cloud Build Service Account:

1. In the Google Cloud console, navigate to **IAM & Admin > IAM**.
2. On the **IAM** page, locate the Cloud Build service account, identifiable with an email address that begins with the **Project ID** and the word **cloudbuild**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, `<project-id>@cloudbuild.gserviceaccount.com`

3. Select the pencil icon to edit the Cloud Build account roles.
4. On the **Edit access to "project-id" page** for the selected principal option, select **ADD ANOTHER ROLE** to add the required roles to your Cloud Build service account one by one and then select **SAVE**.

> **NOTE:**
>
> Enable all the APIs to get the complete list of roles.

After April 29, 2024

Citrix Cloud uses two separate service accounts within the Google Cloud project:

- *Citrix Cloud Service Account*: This service account enables Citrix Cloud to access the Google project, provision, and manage machines. This service account authenticates to Google Cloud using a key generated by Google Cloud.

  You must create this service account manually.

  You can identify this service account with an email address. For example, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.
- *Cloud Compute Service Account*: This service account is provisioned automatically after you enable all the APIs mentioned in Enable Google Cloud APIs. To view all automatically created service accounts, navigate to **IAM & Admin > IAM** in the **Google Cloud** console and select the **Include Google-provided role grants** checkbox. This account has the IAM basic editor role to do the operations. However, if you delete the default permission to have more granular control, you must add **Storage Admin** role that requires the following permissions:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  You can identify this service account by an email address that begins with the **Project ID** and the word **compute**. For example, `<project-id>-compute@developer.gserviceaccount.com.`

  Verify if the service account has been granted the following roles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cloud Build Service Account
- Compute Instance Admin
- Service Account User

CREATE A CITRIX CLOUD SERVICE ACCOUNT

To create a Citrix Cloud Service Account, follow these steps:

1. In the Google Cloud console, navigate to **IAM & Admin > Service accounts**.
2. On the **Service accounts** page, select **CREATE SERVICE ACCOUNT**.
3. On the **Create service account** page, enter the required information, and then select **CREATE AND CONTINUE**.
4. On the **Grant this service account access to project** page, click the **Select a role** drop-down menu and select the required roles. Click **+ADD ANOTHER ROLE** if you want to add more roles.

   Each account (personal or service) has various roles defining the management of the project. Grant the following roles to this service account:

   - Compute Admin
   - Storage Admin
   - Cloud Build Editor
   - Service Account User
   - Cloud Datastore User
   - Cloud KMS Crypto Operator

   The Cloud KMS Crypto Operator requires the following permissions:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

   NOTE:

   Enable all the APIs to get the complete list of roles available while creating a new service account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **CONTINUE**
6. On the **Grant users access to this service account** page, add users or groups to grant them access to perform actions in this service account.
7. Click **DONE**.
8. Navigate to the IAM main console.
9. Identify the service account created.
10. Validate the roles are assigned successfully.

Considerations:

When creating the service account, consider the following:

- The steps **Grant this service account access to project** and **Grant users access to this service account** are optional. If you choose to skip these optional configuration steps, the newly created service account does not display in the **IAM & Admin > IAM** page.
- To display roles associated with a service account, add the roles without skipping the optional steps. This process ensures that roles appear for the configured service account.

CITRIX CLOUD SERVICE ACCOUNT KEY

The Citrix Cloud Service Account key is required for creating a connection in Citrix DaaS. The key is contained in a credential file (.json). The file is automatically downloaded and saved to the **Downloads** folder after you create the key. When you create the key, be sure to set the key type to JSON. Otherwise, Studio cannot parse it.

To create a Service Account Key, navigate to **IAM & Admin > Service accounts** and click the email address of the Citrix Cloud Service Account. Switch to the **Keys** tab and select **Add Key > Create new key**. Make sure to select **JSON** as the key type.

TIP:

Create keys using the **Service accounts** page in the Google Cloud console. We recommend that you change keys regularly for security purposes. You can provide new keys to the Citrix Virtual Apps and Desktops application by editing an existing Google Cloud connection.

ADD ROLES TO THE CITRIX CLOUD SERVICE ACCOUNT

To add roles to the Citrix Cloud Service Account:

1. In the Google Cloud console, navigate to **IAM & Admin > IAM**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the **IAM > PERMISSIONS** page, locate the service account you created, identifiable with an email address.

   For example, `<my-service-account>@<project-id>.iam.gserviceaccount.com`

3. Select the pencil icon to edit the access to the principal of the service account.
4. On the **Edit access to "project-id"** page for the selected principal option, select **ADD ANOTHER ROLE** to add the required roles to your service account one by one and then select **SAVE**.

ADD ROLES TO THE CLOUD COMPUTE SERVICE ACCOUNT

To add roles to the Cloud Compute Service Account:

1. In the Google Cloud console, navigate to **IAM & Admin > IAM**.
2. On the **IAM** page, locate the Cloud Compute Service Account, identifiable with an email address that begins with the **Project ID** and the word **compute**.

   For example, `<project-id>-compute@developer.gserviceaccount.com`

3. Select the pencil icon to edit the Cloud Build account roles.
4. On the **Edit access to "project-id" page** for the selected principal option, select **ADD ANOTHER ROLE** to add the required roles to your Cloud Build service account one by one and then select **SAVE**.

   NOTE:

   Enable all the APIs to get the complete list of roles.

Storage permissions and bucket management

Citrix DaaS improves the process of reporting cloud build failures for the Google Cloud service. This service runs builds on the Google Cloud. Citrix DaaS creates a storage bucket named `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` where the Google Cloud services captures build log information. An option is set on this bucket that deletes the contents after a period of 30 days. This process requires that the service account used for the connection has Google Cloud permissions set to `storage.buckets.update`. If the service account does not have this permission, Citrix DaaS ignores errors and proceeds with the catalog creation process. Without this permission, the size of the build logs increases and requires manual cleanup.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable private Google access

When a VM lacks an external IP address assigned to its network interface, packets are only sent to other internal IP addresses destinations. When you enable private access, the VM connects to the set of external IP addresses used by the Google API and associated services.

NOTE:

Whether private Google access is enabled, all VMs that are with and without public IP addresses, must be able to access Google Public APIs, especially if third-party networking appliances have been installed in the environment.

To ensure that a VM in your subnet can access the Google APIs without a public IP address for MCS provisioning:

1. In Google Cloud, access the **VPC network configuration**.
2. Identify the subnets used or the Citrix® environment in the **Subnets in current project** tab.
3. Click the name of the subnets and enable **Private Google Access**.

For more information, see Configuring Private Google Access.

IMPORTANT:

If your network is configured to prevent VM access to the internet, ensure that your organization assumes the risks associated with enabling Private Google access for the subnet to which the VM is connected.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to Google cloud environments.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HPE Moonshot virtualization environments

Citrix DaaS™ manages your HPE Moonshot workloads through a Citrix-managed HPE Moonshot plug-in present in the DaaS control plane. With this plug-in, you can create connections to your HPE Moonshot chassis, create catalogs, and power manage machines in the catalog.

Key steps

1. Set up your HPE environments.
2. Create a connection to the HPE Moonshot chassis.
3. Create a machine catalog.

   NOTE:

   Before creating a catalog, ensure to have one or more HPE Moonshot cartridge nodes and install VDAs on those nodes. You can consider the HPE Moonshot chassis as the hypervisor and the cartridge nodes as VMs.

4. Create a delivery group.
5. Migrate the rest of unmanaged HPE Moonshot nodes to the managed catalog or delivery group.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine that will deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to HPE Moonshot.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

Microsoft Azure Resource Manager virtualization environments

When using the Microsoft Azure Resource Manager to provision virtual machines in your Citrix DaaS™ deployment, get familiar with the following:

- What is Microsoft Entra ID?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Integrating Microsoft Entra ID with applications getting started guide
- Application and service principal objects in Microsoft Entra ID
- Managed identities for Azure resources

To set up your Microsoft Azure Resource Manager, see Set up resource location.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to Microsoft Azure.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs
- CTX219211: Set up a Microsoft Entra ID account
- CTX219243: Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271: Deploy hybrid cloud using site-to-site VPN

Microsoft SCVMM virtualization environments

Follow this guidance if you use Hyper-V with the Microsoft System Center Virtual Machine Manager (VMM) to provide virtual machines.

See System requirements for a list of supported VMM versions.

You can use Machine Creation Services™ or Citrix Provisioning (formerly Provisioning Services) to provision:

- Generation 1 Desktop or Server OS VMs
- Generation 2 Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10, and Windows 11 VMs (with or without secure boot)

Install and configure a hypervisor

Install the Microsoft Hyper-V role and VMM on your servers.

Verify the following account information:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In Studio, the account you specify when creating a connection must be a VMM administrator or VMM delegated administrator for the relevant Hyper-V machines. If this account has only the delegated administrator role in VMM, the storage data is not listed in Studio during the connection creation process.

Your user account must also be a member of the administrators local security group on each Hyper-V server to support VM lifecycle management (such as VM creation, update, and deletion).

In large deployments where a single SCVMM manages multiple clusters in different data centers, you can limit the host groups scope of the admins.

To limit the host groups scope, use the delegated admin role in the Microsoft System Center Virtual Machine Manager (VMM) console.

1. On **Create User Roles Wizard**, select **Fabric Administrator** (delegated administrator) as a user role.
2. In **Members**, add the user account in the Active Directory that you want to use as delegated admin.
3. In **Scope**, select the host groups you want the delegated admin to have access to.
4. Create a new **Run As Account** using delegated admin user credentials. Use these credentials to create a hypervisor connection later. Do not use the main administrator role accounts.

Install the VMM console

Install a System Center Virtual Machine Manager console on each server having a Citrix Cloud Connector.

The console version must match the management server version. Although an earlier console can connect to the management server, provisioning VDAs fails if the versions differ.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to Microsoft System Center Virtual Machine Manager.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Create machine catalogs

Nutanix virtualization environments

Connect Citrix DaaS™ to Nutanix AHV clusters through Nutanix Prism Central using Nutanix AHV Prism Central host connection. This host connection:

- Supports machine catalogs with both power managed and MCS provisioned VDAs.
- Enables MCS master image sharing across AHV clusters using template versions.
- Simplifies certificate trust on host connection.
- Eliminates the need of Nutanix plug-in installation on Cloud Connectors.

See Nutanix Prism Central on AHV.

You can also use Nutanix Prism Element on AHV using Nutanix Acropolis as the host connection to provide VMs in your Citrix DaaS deployment. However, this setup process requires installing and registering the Nutanix plug-in in your Citrix DaaS environment. See Nutanix Prism Element on AHV.

For more information on the Nutanix Acropolis MCS plug-in Installation guide, see Nutanix Support Portal.

Nutanix Prism Central on AHV

Citrix has developed and maintains a plug-in that integrates Citrix with Nutanix Prism Central on AHV. This plug-in is integrated with Citrix Delivery Controllers, eliminating the need for separate plug-in installations.

The Nutanix AHV Prism Central plug-in is pre-installed on Delivery Controllers managed by Citrix in Citrix DaaS, eliminating the need for separate installation on Cloud Connectors. For information on Citrix-managed components and services, see Components and services managed by Citrix.

Prerequisites

You need the following for Nutanix AHV Prism Central:

- Prism Central version pc.2025.2 or later. Refer to Supported Hypervisors for Citrix Virtual Apps and Desktops (MCS) and Citrix Provisioning (PVS) for detailed supported Prism Central versions.
- AOS version 7.3 or later for the Nutanix AHV clusters.
- Nutanix AHV clusters must register to the Prism Central.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Citrix administrator account must have sufficient permissions to create host connections, machine catalogs, and delivery groups. For more information, see Configure Delegated Administration.
- Citrix Cloud™ communicates with Nutanix Prism Central through the Cloud Connector. Therefore, the Nutanix Prism Central instance must be accessible from the Cloud Connector.

Limitations in the feature

Due to Nutanix Prism and API limitation, power actions like Guest Reboot or Guest Shutdown might fail for a Windows VM. To resolve this issue, we recommend following Nutanix instructions in the document Power actions initiated from Prism or API might fail for Windows VMs to apply settings on VDAs.

Key steps

1. Set up your Nutanix virtualization environments. For information, see Add a resource type or Activate an unused domain.
2. Create a connection to the Nutanix AHV Prism Central
3. Create a machine catalog using Nutanix machine template version.

Nutanix Prism Element on AHV

Nutanix Prism Element on AHV requires installing the Nutanix plug-in on all Cloud Connectors where Citrix DaaS must create a host connection to the resource location that has a Nutanix hypervisor.

Key steps

1. Install and register the Nutanix plug-in.
2. Set up your Nutanix virtualization environments. For information, see Add a resource type or Activate an unused domain.
3. Create a connection.
4. Create a machine catalog.

Install and register the Nutanix plug-in

Complete the procedure to install and register the Nutanix plug-in on all your Cloud Connectors. For information about installing the Nutanix plug-in, see the Nutanix Documentation site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing a connection, see Connection to Nutanix.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

Nutanix cloud and partner solutions

Nutanix AHV Prism Central

Citrix DaaS™ supports Nutanix Cloud Clusters (NC2) in the following cloud hypervisors for Citrix-managed Nutanix AHV Prism Central plug-in.

- Amazon Web Services (AWS)
- Microsoft Azure

Nutanix Cloud Clusters

Citrix DaaS supports Nutanix Cloud Clusters on AWS and Azure. Nutanix clusters simplify how applications are run on private or multiple public clouds.

For more information on setting up NC2, see:

- Nutanix Cloud Clusters on AWS Deployment and User Guide
- Nutanix Cloud Clusters on Azure Deployment and User Guide.

Requirements

You need the following accounts to use NC2:

- A Nutanix account
- For AWS: An AWS account with the following permissions.
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For Azure:
  - A valid “NC2 on Azure” license
  - An Azure account that includes one of the following roles:
    - Global Administrator
    - Cloud Application Administrator
    - Application Administrator
    - all the permissions

Permissions for NC2 on Azure

```
Microsoft.Compute/register/action

Microsoft.Compute/availabilitySets/write

Microsoft.Compute/availabilitySets/delete

Microsoft.Compute/disks/read

Microsoft.Compute/disks/write

Microsoft.Compute/disks/delete

Microsoft.Compute/locations/usages/read

Microsoft.Compute/availabilitySets/read

Microsoft.Compute/virtualMachines/*

Microsoft.Compute/snapshots/*

Microsoft.Compute/images/*

Microsoft.Network/register/action

Microsoft.Network/natGateways/*

Microsoft.Network/networkInterfaces/*

Microsoft.Network/networkSecurityGroups/*
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Microsoft.Network/publicIPAddresses/*

Microsoft.Network/virtualNetworks/*

Microsoft.Network/locations/usages/read

Microsoft.Storage/register/action

Microsoft.Storage/checknameavailability/read Microsoft.Storage/locations/
checknameavailability/read Microsoft.Storage/locations/usages/read

Microsoft.Storage/storageAccounts/write

Microsoft.Storage/storageAccounts/read

Microsoft.Storage/storageAccounts/delete Microsoft.Storage/
storageAccounts/blobServices/containers/clearLegalHold/action
Microsoft.Storage/storageAccounts/blobServices/containers/delete
Microsoft.Storage/storageAccounts/blobServices/containers/lease/action

Microsoft.Storage/storageAccounts/blobServices/containers/ read
Microsoft.Storage/storageAccounts/blobServices/containers/ write
Microsoft.Storage/storageAccounts/blobServices/read Microsoft.Storage/
storageAccounts/blobServices/write Microsoft.Storage/storageAccounts/
listAccountSas/action Microsoft.Storage/storageAccounts/listkeys/action
Microsoft.Storage/storageAccounts/listServiceSas/action Microsoft.Storage/
storageAccounts/regeneratekey/action Microsoft.Storage/storageAccounts/
revokeUserDelegationKeys/action Microsoft.ResourceHealth/
AvailabilityStatuses/read Microsoft.ResourceHealth/events/read

Microsoft.ResourceHealth/AvailabilityStatuses/current/read

Microsoft.ManagedIdentity/userAssignedIdentities/* Microsoft.Resources/
subscriptions/locations/read Microsoft.Resources/subscriptions/
resourceGroups/read Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourcegroups/deployments/read

Microsoft.Resources/subscriptions/resourcegroups/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/resources/read
Microsoft.Resources/subscriptions/tagNames/read Microsoft.Resources/
subscriptions/tagNames/write Microsoft.Resources/subscriptions/tagNames/
delete Microsoft.Resources/subscriptions/tagNames/tagValues/write
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Microsoft.Resources/subscriptions/tagNames/tagValues/read
Microsoft.Resources/subscriptions/tagNames/tagValues/delete
Microsoft.Resources/tags/read

Microsoft.Resources/tags/write

Microsoft.Resources/tags/delete

Microsoft.Resources/providers/read

Microsoft.Compute/sshPublicKeys/read

Microsoft.Compute/sshPublicKeys/write

Microsoft.Compute/sshPublicKeys/delete Microsoft.Compute/sshPublicKeys/
generateKeyPair/action Microsoft.Nutanix/Interfaces/read

Microsoft.Nutanix/Interfaces/write

Microsoft.Nutanix/Interfaces/delete

Microsoft.Nutanix/Nodes/read

Microsoft.Nutanix/Nodes/write

Microsoft.Nutanix/Nodes/delete

Microsoft.Nutanix/register/action

Microsoft.Network/virtualHubs/*

Microsoft.Network/routeTables/read

Microsoft.Network/routeTables/write

Microsoft.Network/routeTables/delete

Microsoft.Network/routeTables/join/action

Microsoft.Network/routeTables/routes/read Microsoft.Network/routeTables/
routes/write Microsoft.Network/routeTables/routes/delete
Microsoft.CostManagement/query/read

Microsoft.CostManagement/views/read Microsoft.CostManagement/
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
externalSubscriptions/query/read Microsoft.CostManagement/
externalSubscriptions/dimensions/read Microsoft.CostManagement/
externalSubscriptions/read Microsoft.CostManagement/
externalBillingAccounts/forecast/read

Microsoft.CostManagement/externalBillingAccounts/read

Microsoft.CostManagement/externalBillingAccounts/query/read
Microsoft.CostManagement/externalBillingAccounts/ externalSubscriptions/
read Microsoft.CostManagement/externalSubscriptions/forecast/read
Microsoft.CostManagement/operations/read Microsoft.CostManagement/
forecast/read

Microsoft.Network/virtualWans/write

Microsoft.Network/virtualWans/read

Microsoft.Network/virtualWans/delete Microsoft.Network/virtualWans/
virtualHubs/read Microsoft.Network/virtualWans/join/action
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ read
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ write
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ delete
Microsoft.Network/privateEndpoints/pushPropertiesToResource/ action
Microsoft.Network/privateEndpoints/read

Microsoft.Network/privateEndpoints/write Microsoft.Network/
privateEndpoints/delete Microsoft.Network/privateDnsZones/read
Microsoft.Network/privateDnsZones/delete Microsoft.Network/
privateDnsZones/join/action Microsoft.Network/privateDnsZones/write
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/ write

Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
deleteBlobVersion/action

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/
read Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/
read
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write
Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/write
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
modifyPermissions/action
```

Create a Nutanix Cluster

1. Log in to your Nutanix account.
2. Navigate to the Nutanix cluster option, and click **Launch**. The **Nutanix Console** opens. For more information:
   - Get Started with Nutanix Cluster on AWS
   - Nutanix Cloud Clusters on Microsoft Azure
3. Select the option to create a new VPC.

Once the cluster is created, retrieve the address of the Nutanix Prism.

TROUBLESHOOTING

The cluster creation process might fail with the following errors:

- **Cluster failed to create within a given time. Deleting cluster**
- **Host Nutanix Cluster - Node XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error**.
- **Host Nutanix Cluster - Node XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info**

If the cluster fails to create, then try to recreate one in a different region. Make sure to delete the Nutanix CloudFormation Stack (CFS) before retrying.

NOTE:

In addition to other resources, the Nutanix CFS creates:

- One VPC named Nutanix Cluster xxxxxxxxxxxx 10.0.0.0/16
- Two subnets 10.0.128.0/24 and 10.0.129.0/24
- One Internet gateway
- One NAT gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Retrieve the Prism server address

1. Register the NC2 cluster with the Prism Central server. See Registering a Cluster with Prism Central.
2. Use the host name or IP address of the Prism Central server as the address.

NC2 for Nutanix Prism Element

Citrix DaaS supports Nutanix Cloud Clusters (NC2) in the following cloud hypervisor for the Nutanix Prism Element plug-in.

- Amazon Web Services (AWS)

Nutanix Cloud Clusters on AWS

For more information on Nutanix Cloud Clusters on AWS, see Nutanix Cloud Clusters on AWS Deployment and User Guide.

TIP:

This support provides the same functionality as a Nutanix on-premises cluster. Only a single cluster is supported, the *Prism Element*. For more information, see here.

You need the following accounts to use NC2 on AWS:

- A Nutanix account
- An AWS account with the following permissions:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

For creating a Nutanix Cluster and troubleshooting if cluster creation fails, see Create a Nutanix Cluster and Troubleshooting.

Once the cluster is created, retrieve the address of the **Nutanix Prism**:

Retrieve the prism server address

1. Go to the **Nutanix Console**.
2. In the upper right on the console, hover over the link **Launch Prism Element** and copy the URL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to Nutanix cloud and partner solutions.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

Red Hat OpenShift virtualization environments

Citrix® manages your Red Hat OpenShift workloads through a Citrix-managed OpenShift plug-in. With this plug-in, you can create hosting connections and hosting units to your OpenShift cluster, create catalogs, and power manage machines in the catalog.

The following configurations are supported:

- Networking options:
  - Linux Bridge and OVS Bridge: Available for cluster networking.
- Storage options:
  - Local storage: Supported for on-node persistent storage.
  - NetApp storage: Supported for enterprise-grade external storage integration.

Key steps

- Set up your Red Hat OpenShift environment.
- Create a connection and a resource to the OpenShift cluster.
- Create a machine catalog.
- Create a delivery group.

Set up your Red Hat OpenShift environment

1. *Create an OpenShift cluster and obtain the cluster API address*: In the OpenShift console, after setting up a cluster, navigate to **Home > Overview > Details**, and get the cluster API address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. *Create a service account and obtain the service account token using the OpenShift command-line interface (CLI) (oc command)*: The service account token is the authentication credential associated with the service account. The service account is used to authenticate the OpenShift plug-in with OpenShift. Each service account is associated with one namespace.
3. *Configure permissions for the service account*: A service account can have multiple roles, and each role consists of permissions that define what actions the OpenShift Plugin can perform on which resources. The roles are bound through **Role Bindings**, and there are two types of **Role Bindings**:
    a. **Cluster-wide Role Binding**: used for receiving events from OpenShift. Namespace-bound Role Binding: used for managing VMs in a specific namespace.
    b. **Namespace-bound Role Binding**: used for managing VMs in a specific namespace.
4. *Create a namespace (Project)*: Namespace in OpenShift is an isolated environment that groups resources like VMs or networks, allowing better organization and access control. **Namespace** is the Kubernetes term, while **Project** is the OpenShift term. From the OpenShift Plugin perspective, they are the same. A namespace is required to deploy the VMs. Use the OpenShift console or OpenShift Container Platform CLI to create the name space.
5. *Create one network attachment definition under the target namespace*: Network attachment definitions specify the networking configuration for VMs running in OpenShift. Under **Networking > NetworkAttachmentDefinitions**, you can see the Network Attachment Definitions for each Namespace.
6. *Configure the storage classes*: Storage classes define how VM storage is allocated. Under **Storage > StorageClass**, you can configure and see the list of storage providers.

Create a service account

1. Download and unzip oc Command Line Tool.
2. Access the OpenShift Console using your login ID.
3. Click your user profile and click **Copy login command**.
4. Click **Display Token** and copy the token.
5. Run the login command using oc Command Line. Example:

```
.\oc.exe login --token=<token> --server=<server address>
```

6. Create a service account.
    - If you want to create the service account under the default namespace, run:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
.\oc.exe create sa <service account name>
```

- If you want to create the service account under your own namespace, run:

```
.\oc.exe create sa <service account name> -n mynamespace
```

7. Create a `YAML` file for secret. Example:

- If you create the service account under the default namespace:

```
apiVersion: v1

kind: Secret

metadata:

name: service account name

annotations:

kubernetes.io/service-account.name: service account name

type: kubernetes.io/service-account-token
```

- If you create the service account under your own namespace:

```
apiVersion: v1

kind: Secret

metadata:

name: service account name

namespace: mynamespace

annotations:

kubernetes.io/service-account.name: service account name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
type: kubernetes.io/service-account-token
```

8. Apply the YAML.

```
.\oc.exe apply -f <yamlFile.yaml>
```

NOTE:

The `oc` describes the secret to get the token. The token is used as a password.

Create roles and role bindings for the service account

With the cluster-wide role binding, the service account has permissions to read all VM events across the cluster, allowing the OpenShift plug-in to maintain a single event watcher for all VM-related events. With the namespace role binding the service account has permissions to manage VMs in the target namespace. You can use a script to create roles and bind them to a service account. See `<https://github.com/citrix/citrix-mcs-sdk-samples/tree/main/OpenShift/Hosting%20Connection/Role/>`.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine that will deliver apps or a desktop to your users.
- For creating and managing a connection, see Connection to Red Hat OpenShift

More information

- Create and manage connections and resources
- Create machine catalogs

VMware virtualization environments

Follow this guidance if you use VMware to provide virtual machines.

Install vCenter Server and the appropriate management tools. (No support is provided for vSphere vCenter Linked Mode operation.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

No support is provided for vSphere vCenter Linked Mode operation.

If you plan to use Machine Creation Services™ (MCS), do not disable the Datastore Browser feature in vCenter Server. If you disable this feature, MCS does not work correctly.

To set up your VMware virtualization environments, see Add a resource type or activate an unused domain in Citrix Cloud.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to VMware.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

VMware cloud and partner solutions

Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) supports the following VMware cloud and partner solutions:

- Azure VMware Solution (AVS)
- Google Cloud VMware Engine
- VMware Cloud on Amazon Web Services (AWS)

Use Citrix DaaS™ to migrate VMware based on-premises Citrix workloads to the respective VMware partner solutions.

Azure VMware Solution (AVS) integration

Citrix DaaS supports AVS. AVS provides cloud infrastructure containing vSphere clusters created by Azure infrastructure. Leverage DaaS to use AVS for provisioning your VDA workload in the same way that you would using vSphere in on-premises environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set up the AVS cluster

To enable Citrix DaaS to use AVS, do the following steps in Azure:

- Request a host quota
- Register the `Microsoft.AVS` resource provider
- Verify networking planning checklist
- Network Checklist
- Create an AVS private cloud
- Access the AVS private cloud
- Configure networking for your VMware private cloud in Azure
- Configure DHCP for AVS
- Add a network segment in AVS
- Verify the AVS environment

REQUEST HOST QUOTA FOR AZURE ENTERPRISE AGREEMENT CUSTOMERS

In the Azure portal's **Help + Support** page select **New support request**, and include the following information:

- Issue type: Technical
- Subscription: Select your subscription
- Service:**All services > Azure VMware Solution**
- Resource: General question
- Summary: Need capacity
- Problem type: Capacity Management Issues
- Problem subtype: Customer Request for Additional Host Quota/Capacity

In the **Description** of the support ticket, include the following information in the **Details** tab:

- POC or Production
- Region Name
- Number of hosts
- Any other details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

AVS requires a minimum of three hosts, and recommends that you use redundancy of N+1 hosts.

After specifying details for the support ticket, select **Review + Create** to submit the request to Azure.

REGISTER THE MICROSOFT.AVS RESOURCE PROVIDER

After requesting the host quota, register the resource provider:

1. Sign in to the Azure portal.
2. On the Azure portal menu, select **All services**.
3. In the **All services** menu, enter the subscription, and select **Subscriptions**.
4. Select the subscription from the subscription list.
5. Select **Resource providers** and enter **Microsoft.AVS** in the search bar.
6. If the resource provider is not registered, select **Register**.

NETWORKING CONSIDERATIONS

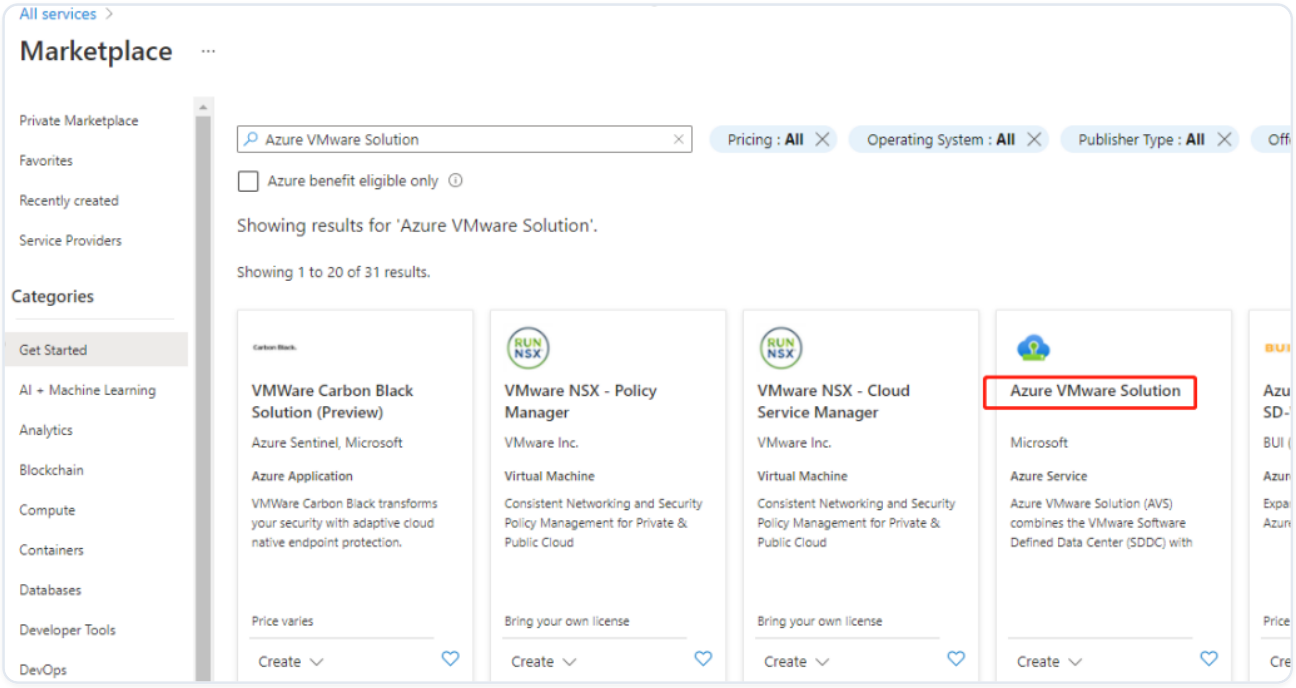
AVS offers networking services requiring specific network address ranges and firewall ports. See Networking planning checklist for Azure VMware Solution for more information.

CREATE AN AVS PRIVATE CLOUD

After considering network requirements for your environment, create an ASV private cloud:

1. Sign in to the Azure portal.
2. Select **Create a new resource**.
3. In the **Search the Marketplace** text box type, *Azure VMware Solution*, and select **Azure VMware Solution** from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In the **Azure VMware Solution** window:

1. Select **Create**.
2. Go to the **Basics** tab.
3. Enter the values for the fields, using the information in the table below:

FIELD	VALUE
Subscription	Select the subscription that you plan to use for the deployment. All resources in an Azure subscription are billed together.
Resource group	Select the resource group for your private cloud. An Azure resource group is a logical container into which Azure resources are deployed and managed. Alternatively, you can create a new resource group for your private cloud.
Location	Select a location, such as east us. This is the region you defined during the planning phase.
Resource name	Provide the name of your Azure VMware Solution private cloud.
Size of host	Select the size as per your need.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD	VALUE
Number of hosts	Shows the number of hosts allocated for the private cloud cluster. The default value is 3, which can be raised or lowered after deployment.
Address block for private cloud	Provide an IP address block for the private cloud. The CIDR represents the private cloud management network and will be used for the cluster management services, such as vCenter Server and NSX-T Manager. Use /22 address space, for example, 10.175.0.0/22. The address should be unique and not overlap with other Azure Virtual Networks and with on-premises networks.

In the **Create a private cloud** screen:

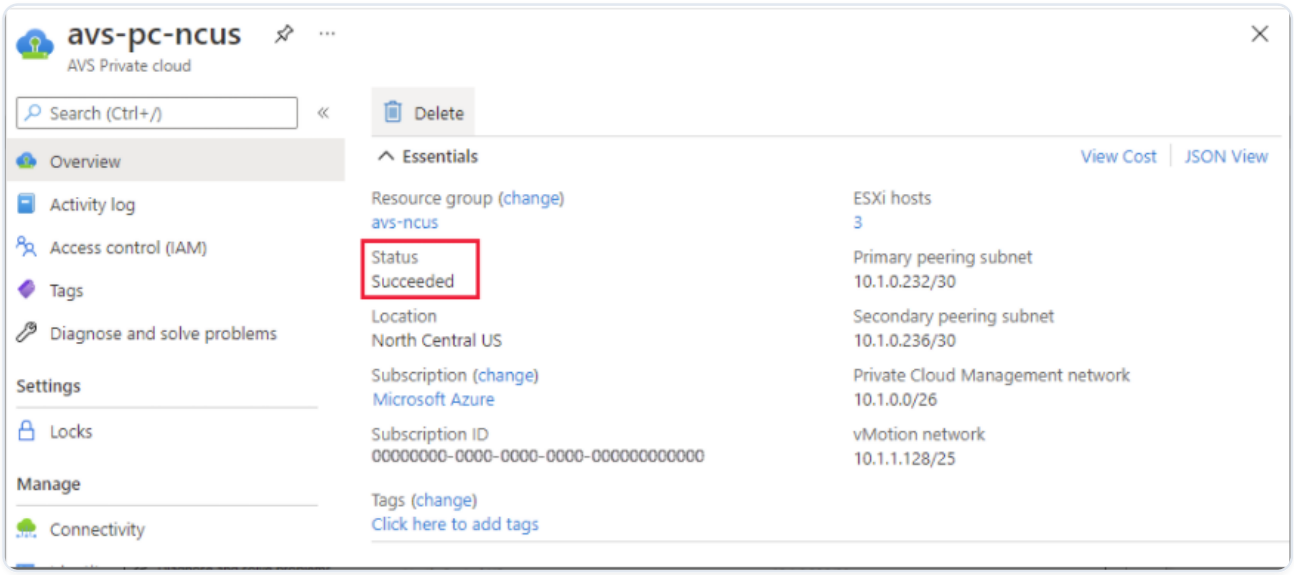
1. In the **Location** field, select the region that has the AVS. The resource group region is the same as the AVS region.
2. In the **Size of host** field, select a size as per your need.
3. Specify an IP address in the **Address Block for private cloud** field. For example, 10.15.0.0/22.
4. Select **Review + Create**.
5. After reviewing the information, click **Create**.

TIP:

Creating a private cloud can take 3–4 hours. Adding a single host to the cluster can take 30–45 minutes.

Verify that the deployment was successful. Navigate to the resource group that you created and select your private cloud. Once the **Status** is **Succeeded** the deployment is complete.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



ACCESS THE AVS PRIVATE CLOUD

Once you have created a private cloud, create a Windows VM and connect to the local vCenter of your private cloud.

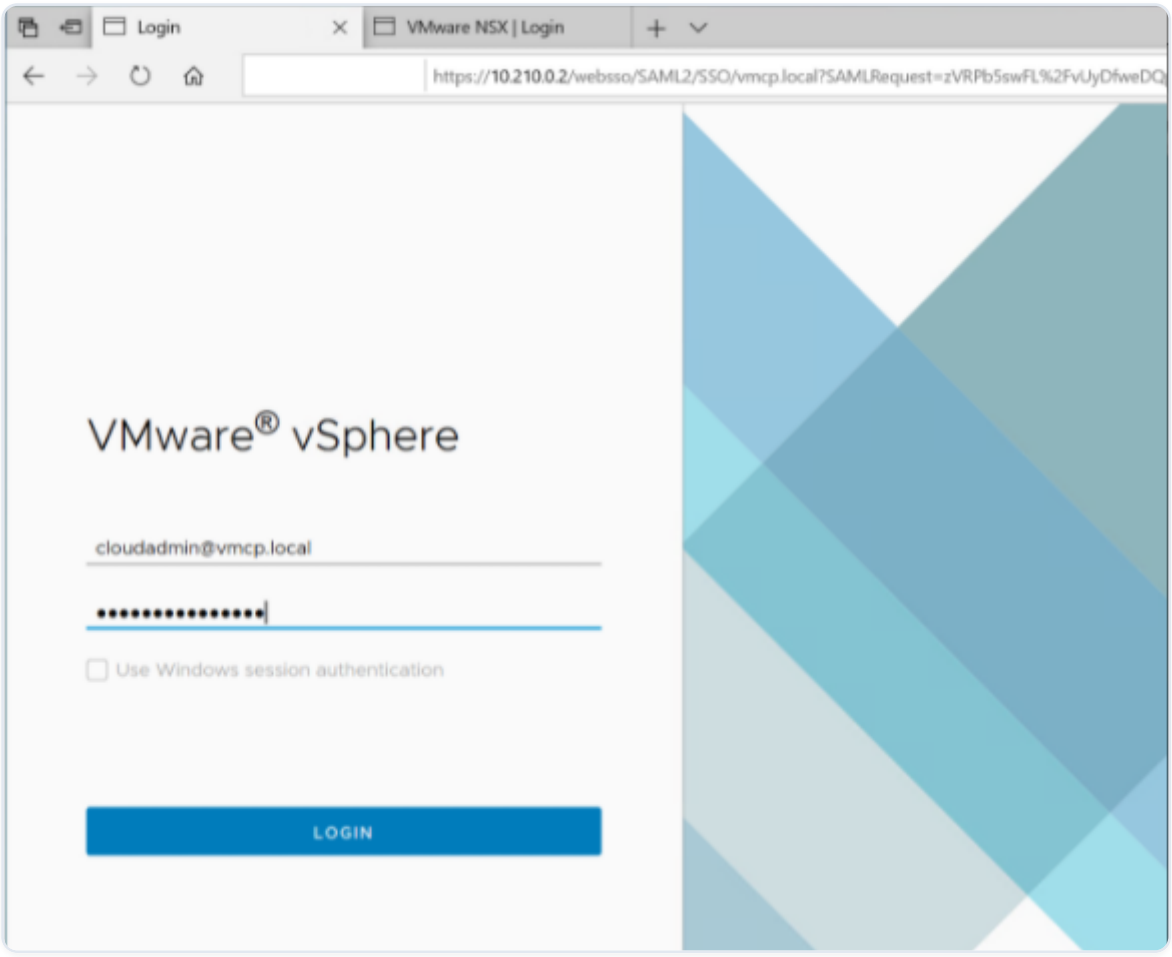
Create a new Windows virtual machine

1. In the resource group, select **+ Add** then search and select **Microsoft Windows 10/11 or Windows Server 2016/2019**.
2. Enter the required information, then select **Review + Create**.
3. Once validation passes, select **Create** to start the virtual machine creation process.

Connect to the local vCenter of your private cloud

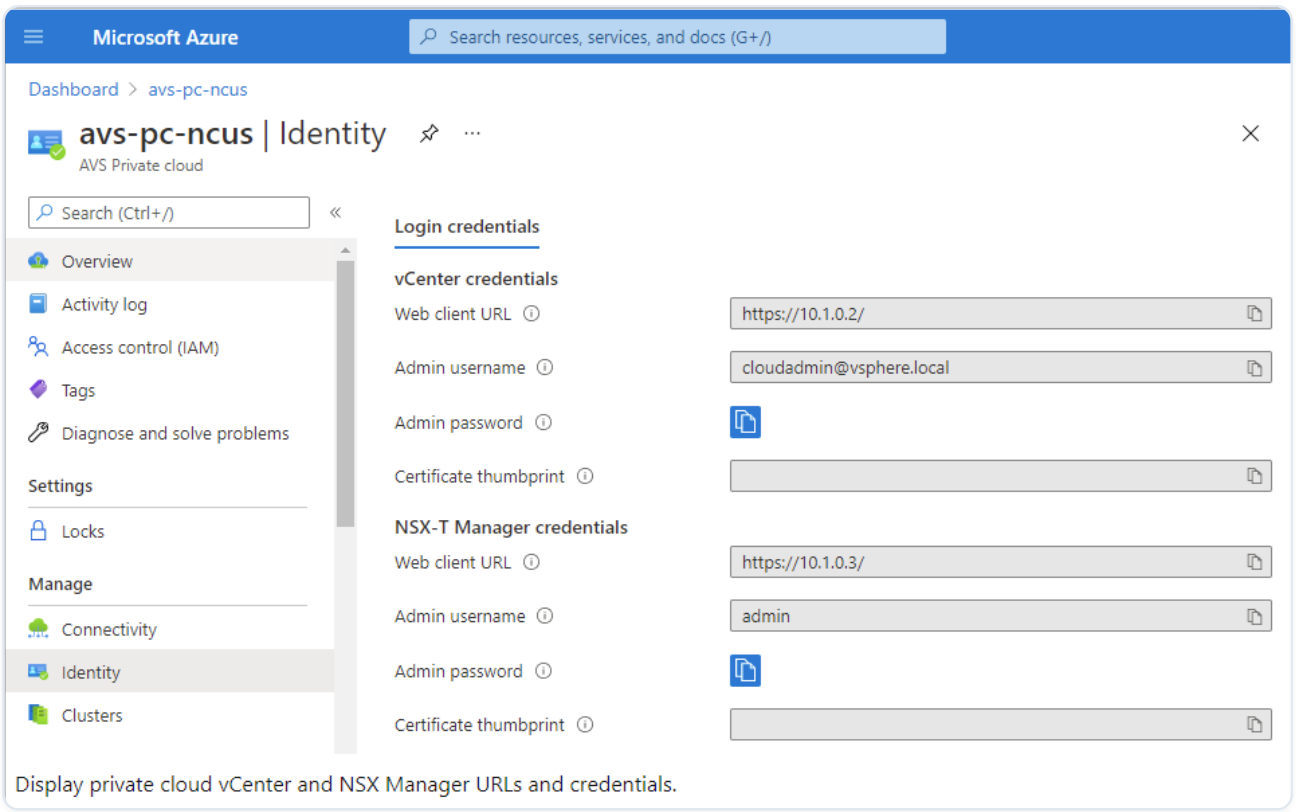
1. Sign in to **vSphere Client with VMware vCenter SSO** as a cloud administrator.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. In the Azure portal, select your private cloud, and then **Manage> Identity**.

The URLs and user credentials for private cloud vCenter and NSX-T Manager appear:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

After confirming URLs and user credentials:

1. Navigate to the VM that you created in the preceding step and connect to the virtual machine.
2. In the Windows VM, open a browser and navigate to the vCenter and NSX-T Manager URLs in two browser tabs. In the vCenter tab, enter the mailto:cloudadmin@vmcp.local user credentials from the previous step.

CONFIGURE NETWORKING FOR YOUR VMWARE PRIVATE CLOUD IN AZURE

After accessing an ASV private cloud, configure networking by creating a virtual network and gateway.

Create a virtual network

1. Sign in to the Azure portal.
2. Navigate to the previously created resource group.
3. Select **+ Add** to define a new resource.
4. In the **Search the Marketplace** text box, type *virtual network*. Find the virtual network resource and select it.
5. On the **Virtual Network** page, select **Create** to set up the virtual network for your private cloud.
6. On the **Create Virtual Network** page, enter the details for your virtual network.
7. On the **Basics** tab, enter a name for the virtual network, select the appropriate region, and click **Next : IP Addresses.**
8. On the **IP Addresses** tab, under IPv4 address space, enter the previously created address.

IMPORTANT:

Use an address that does not overlap with the address space you used when you created your private cloud.

After entering the address space:

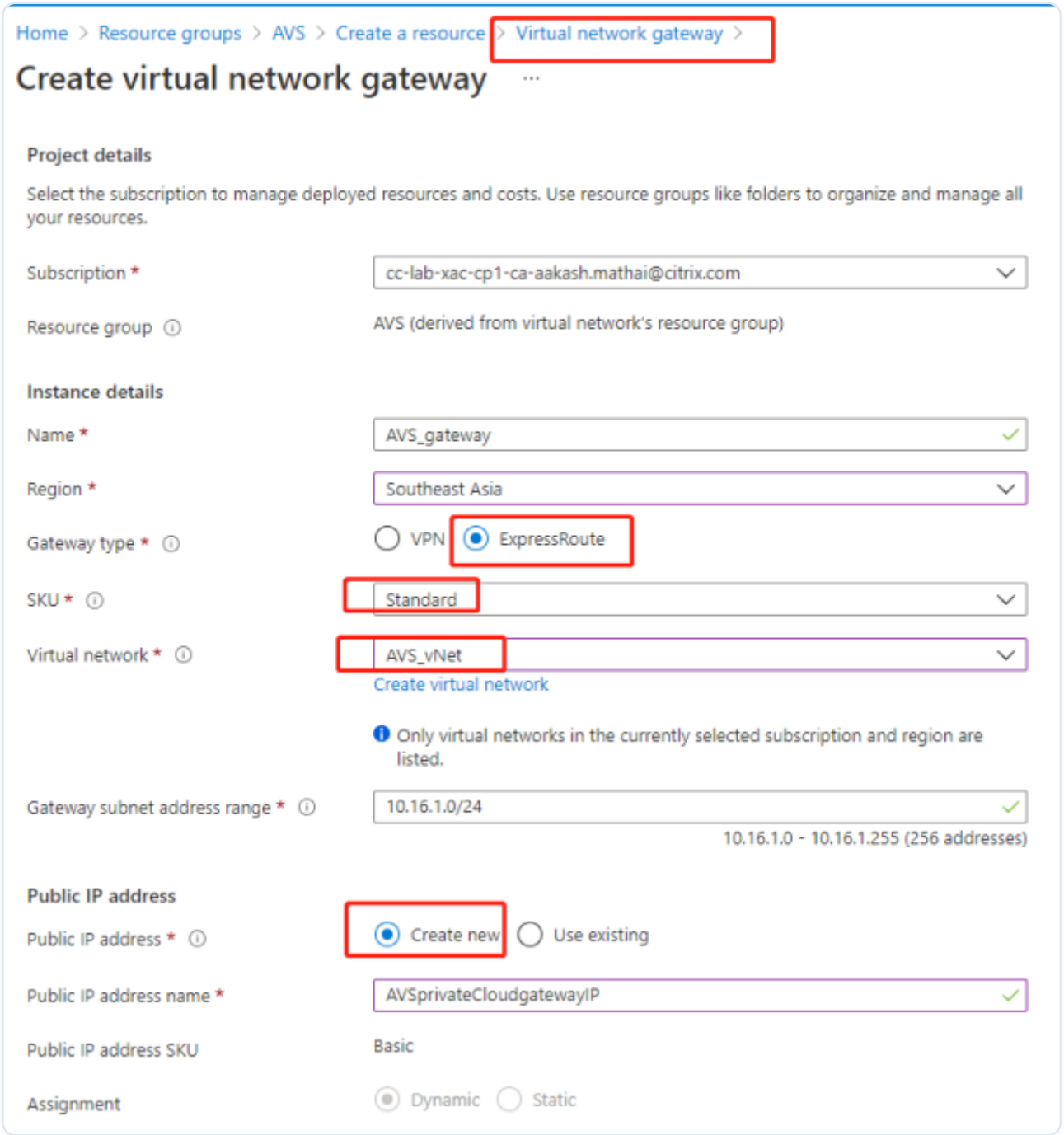
1. Select **+ Add subnet**.
2. On the **Add subnet** page, give the subnet a name and appropriate address range.
3. Click **Add.**
4. Select **Review + create**.
5. Verify the information and click **Create**. Once the deployment is complete, the virtual network appears in the resource group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a virtual network gateway

After creating a virtual network, create a virtual network gateway.

1. In your resource group, select **+ Add** to add a new resource.
2. In the **Search the Marketplace** text box, type *virtual network gateway*. Find the virtual network resource and select it.
3. On the **Virtual Network gateway** page, click **Create**.
4. On the **Basics** tab in the **Create virtual network gateway** page, provide values for the fields.
5. Click **Review + create**.



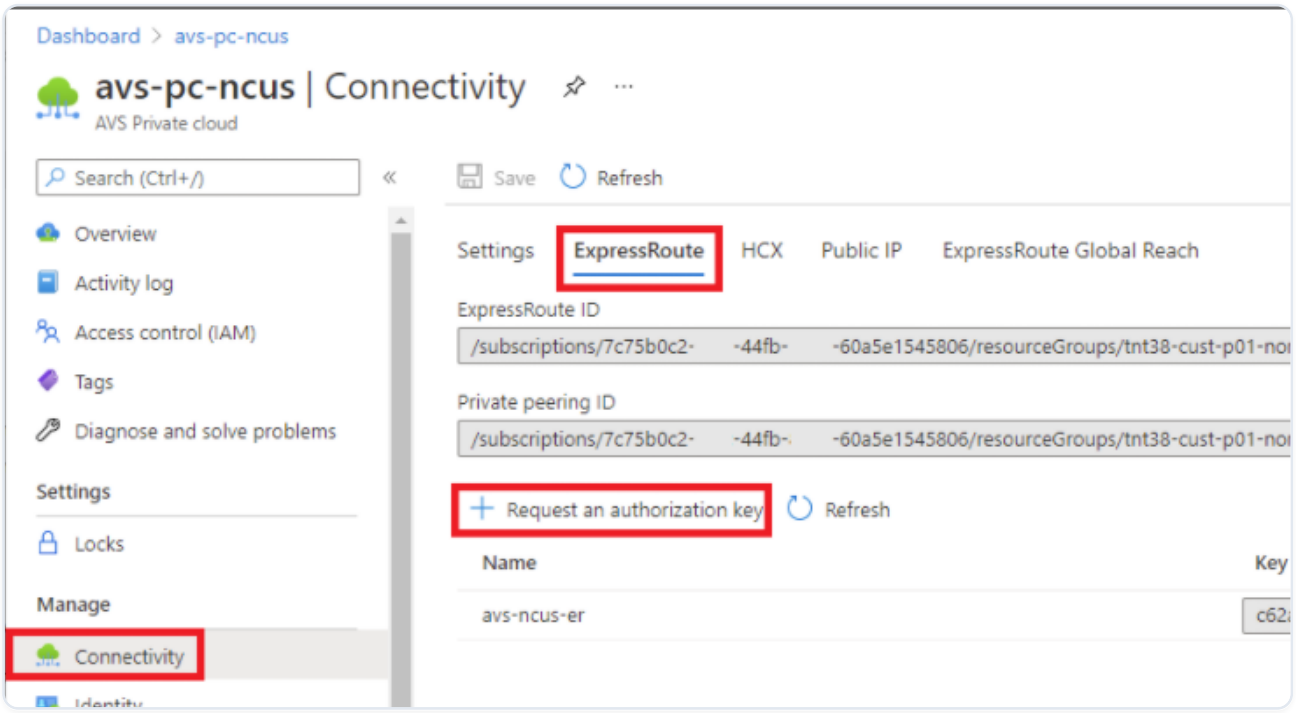
© 1997–2026 Citrix Systems, Inc. All rights reserved.

After reviewing the virtual network gateway configuration, click **Create** to deploy your virtual network gateway. Once the deployment completes, connect your **ExpressRoute** connection to the virtual network gateway containing your Azure AVS private cloud.

CONNECT EXPRESSROUTE TO THE VIRTUAL NETWORK GATEWAY

After deploying a virtual network gateway, add a connection between it and your Azure AVS private cloud:

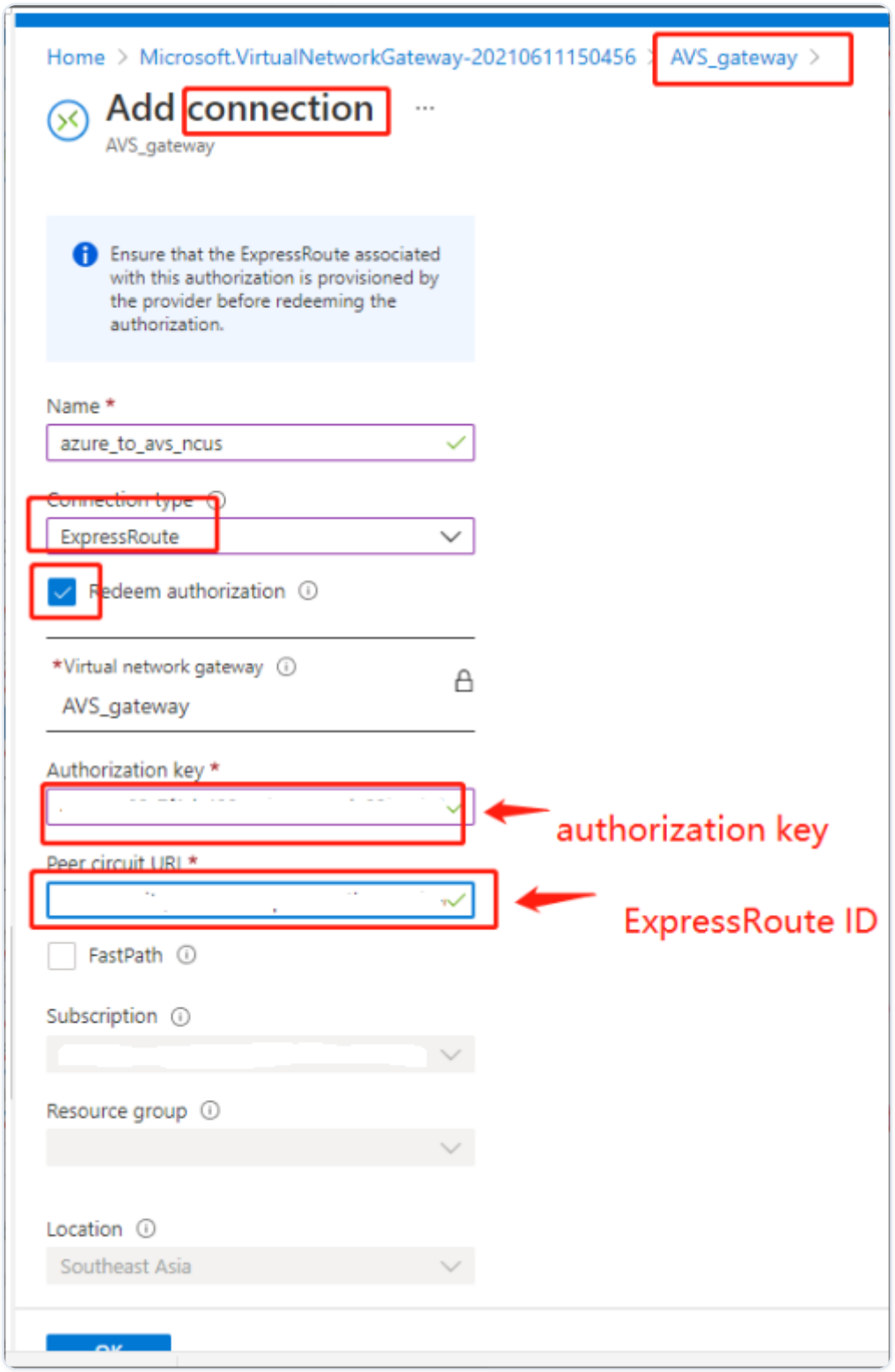
1. Request an ExpressRoute authorization key.
2. In the Azure portal, navigate to the **Azure VMware Solution private cloud**. Select **Manage> Connectivity > ExpressRoute** and then select **+ Request an authorization key.**



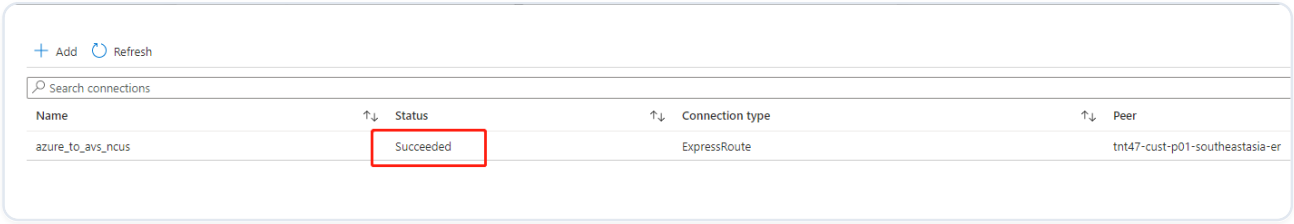
After requesting an authorization key:

1. Enter a name for the key and click **Create**. It may take about 30 seconds to create the key. Once created, the new key appears in the list of authorization keys for the private cloud.
2. Copy the **authorization key** and **ExpressRoute ID**. You'll need them to complete the peering process. The authorization key disappears after some time, so copy it when it appears.
3. Navigate to the **virtual network gateway** you plan to use and select **Connections> + Add**.
4. On the **Add connection** page, provide values for the fields, and select **OK.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The connection is established between your ExpressRoute circuit and your virtual network:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

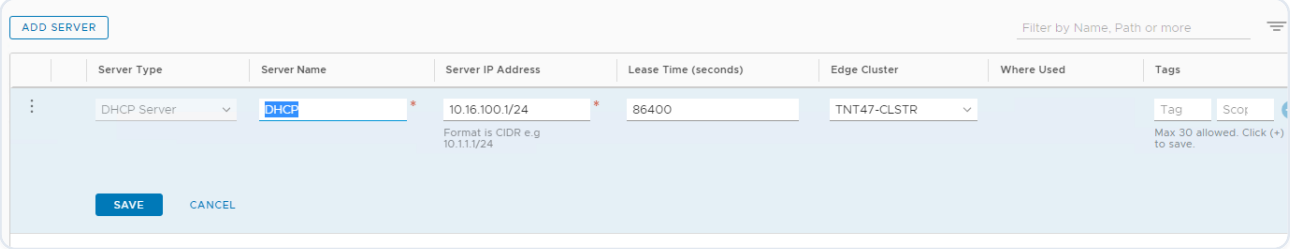
CONFIGURE DHCP FOR AZURE VMWARE SOLUTION

After connecting ExpressRoute to the virtual gateway, configure DHCP.

Use NSX-T to host your DHCP server

In NSX-T Manager:

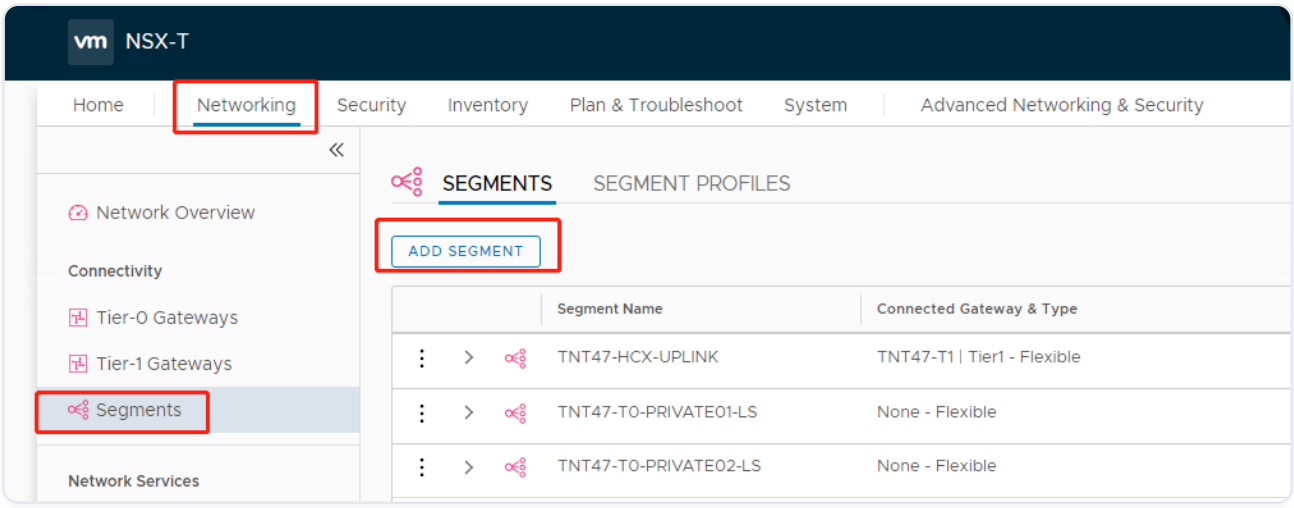
1. Select **Networking> DHCP**, and then select **Add Server**.
2. Select **DHCP** for the **Server Type**, provide the server name and IP address.
3. Click **Save**.
4. Select **Tier 1 Gateways**, select the vertical ellipsis on the Tier-1 gateway, and then select **Edit**.
5. Select **No IP Allocation Set** to add a subnet.
6. Select **DHCP Local Server** for the **Type**.
7. For the **DHCP Server**, select **Default DHCP**, and then click **Save**.
8. Click **Save** again and then select **Close Editing**.



ADD A NETWORK SEGMENT IN THE AZURE VMWARE SOLUTION

After setting up DHCP, add a network segment.

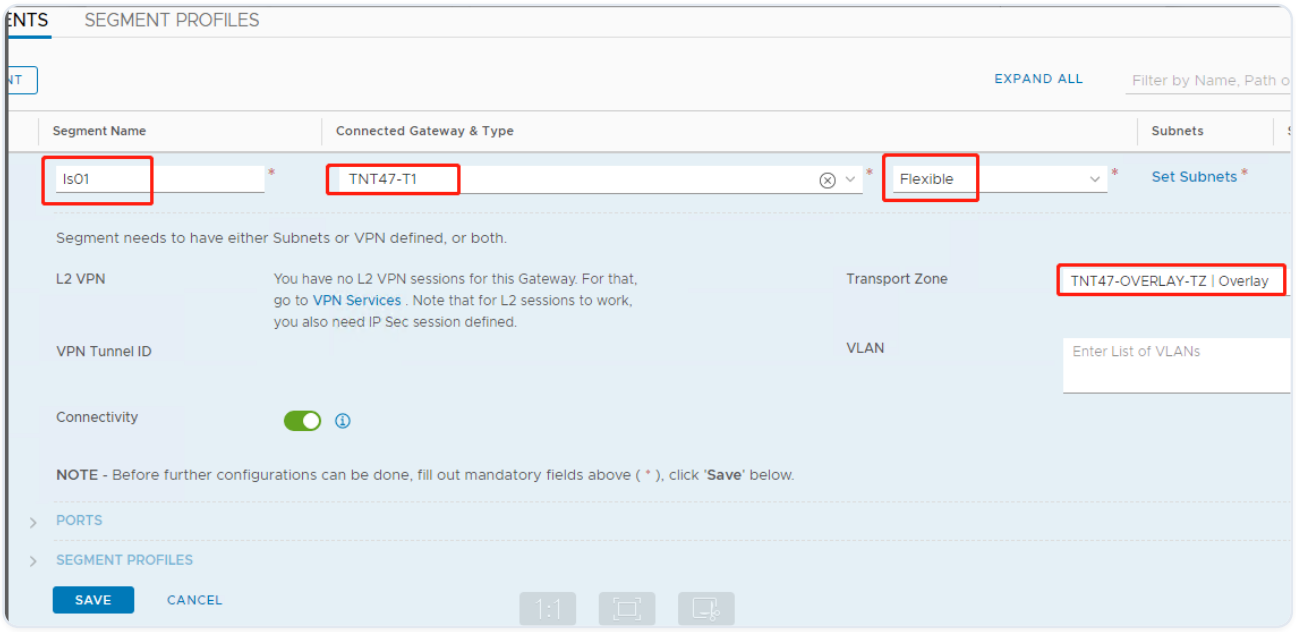
To add a network segment, in NSX-T Manager, select **Networking> Segments**, and then click **Add Segment**.



In the **Segments profile** screen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Enter a **name** for the segment.
2. Select the **Tier-1 Gateway (TNTxx-T1)** as the **Connected Gateway** and leave the **Type** as **Flexible**.
3. Select the pre-configured overlay **Transport Zone(TNTxx-OVERLAY-TZ)**.
4. Click **Set Subnets**.



In the **Subnets** section:

1. Enter the gateway IP address.
2. Select **Add**.

IMPORTANT:

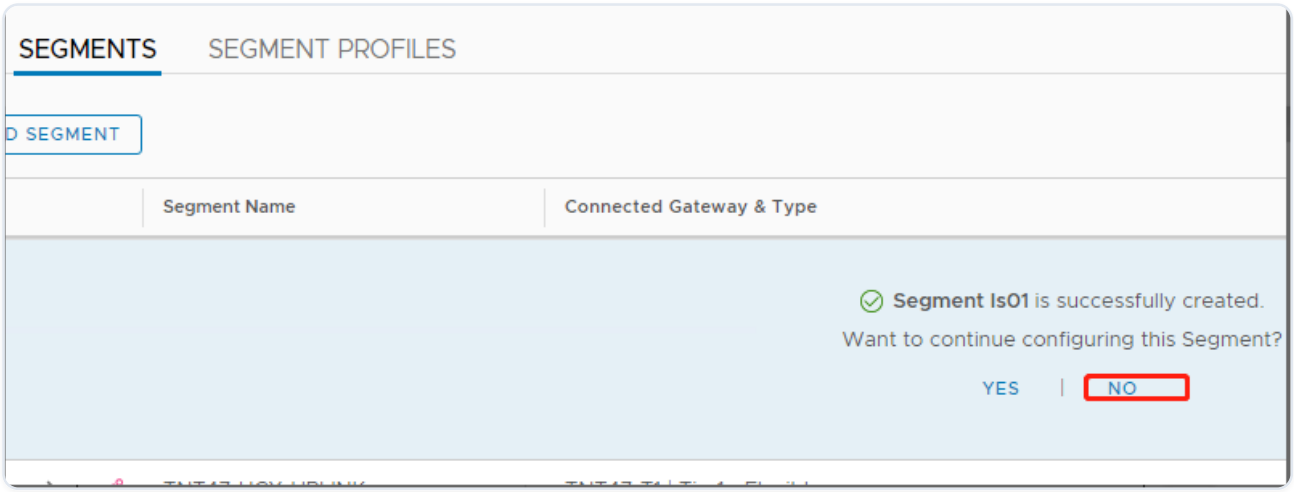
This segment IP address must belong to the Azure gateway IP address, 10.15.0.0/22.

DHCP range must belong to segment IP address:

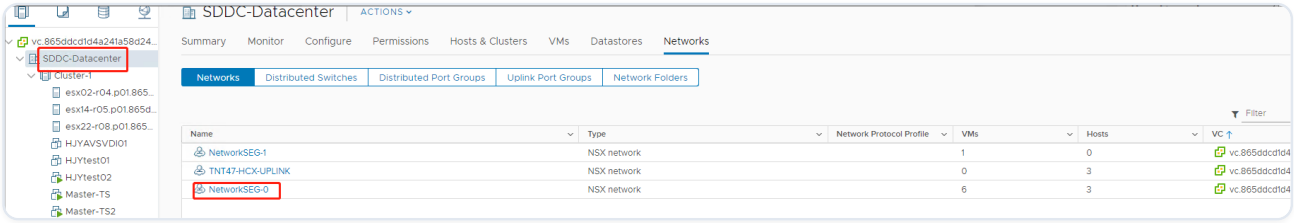


Select **No** to decline the option to continue configuring the segment:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In vCenter, select **Networking > SDDC-Datacenter**:



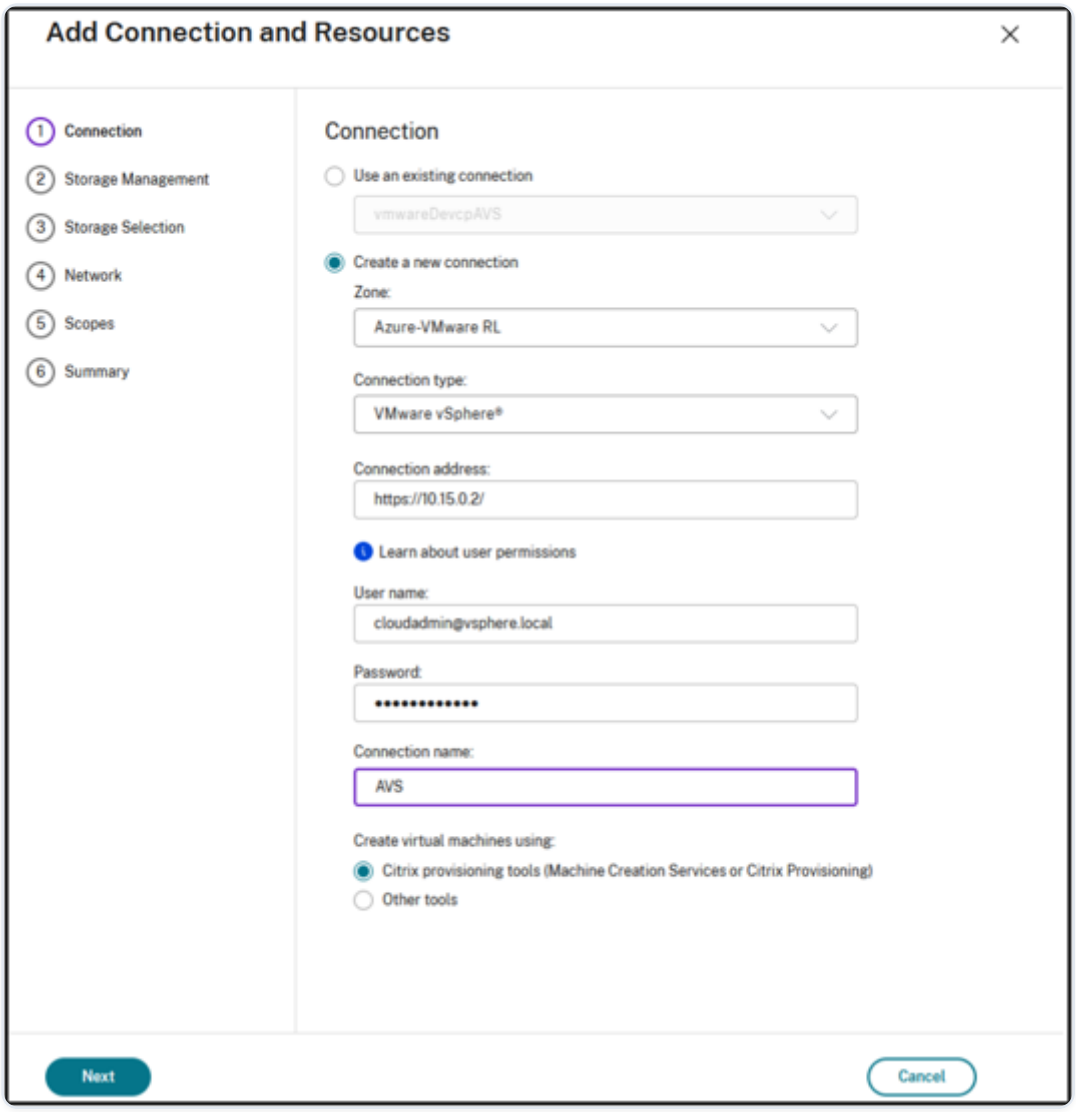
VERIFY THE AVS ENVIRONMENT

Set up resource location for the AVS private cloud and install a pair of cloud connectors.

CREATE THE AVS CONNECTION IN CITRIX STUDIO

1. Create a machine in vCenter and install a pair of Cloud Connectors in the machine. See Configure the instances.
2. From Studio, select Hosting in the left pane.
3. Select the hosting node, and click **Add Connection and Resources**.
4. On the **Connection** screen, select **Create a new Connection**, and the following details:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. Select **Connection type** as **VMware vSphere**.

b. In the **Connection address**, enter the vCenter private IP address.

c. Enter the vCenter credentials.

d. Enter a connection name.

e. Choose the tool to create virtual machines.

5. On the **Network** screen, select the subnet created in the NSX-T server.

6. Complete the wizard.

Google Cloud VMware Engine

Citrix DaaS lets you migrate VMware-based on-premises Citrix workloads to Google Cloud VMware Engine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Google Cloud VMware Engine

The following procedure describes how to acquire and set up cluster on Google Cloud VMware Engine.

ACCESS THE VMWARE ENGINE PORTAL

1. In the **Google Cloud Console**, click the navigation menu.
2. In the **Compute** section, click **VMware Engine** to open VMware Engine in a new browser tab.

REQUIREMENTS TO CREATE FIRST PRIVATE CLOUD

You must have access to Google Cloud VMware Engine, available VMware Engine node quota, and an appropriate IAM role. Set up the following requirements before you continue to create your private cloud:

1. Request API access and node quota. For more information, see Requesting API access and quota.
2. Note the address ranges you want to use for VMware management appliances and the HCX deployment network. For more information, see Networking requirements.

   NOTE:

   The HCX deployment is only applicable to IP Plan version 1.0.

3. Get the VMware Engine Service Admin IAM role.

CREATE YOUR FIRST PRIVATE CLOUD

1. Access the VMware Engine portal.
2. On the VMware Engine Home page, click **Create a private cloud**. The hosting location and hardware node types are listed.
3. Select the number of nodes for the private cloud. At least three nodes are required.
4. Enter a Classless Inter-Domain Routing (CIDR) range for the VMware management network.
5. Enter a CIDR range for the HCX deployment network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

- The CIDR range must not overlap with any of your on-premises or cloud subnets. The CIDR range must be /27 or higher.
- The HCX deployment is only applicable to IP Plan version 1.0.

6. Select **Review and create**.
7. Review the settings. To change any settings, click **Back**.
8. Click **Create** to begin creating the private cloud.

As VMware Engine creates your new private cloud, it deploys several VMware components and sets up initial Autoscale™ policies for clusters in the private cloud. Private cloud creation can take 30 minutes to 2 hours. After the provisioning is complete, you receive an email.

SET UP GOOGLE CLOUD VMWARE ENGINE VPN GATEWAY

To establish an initial connectivity to Google Cloud VMware Engine, you can use a VPN gateway. This is an OpenVPN-based client VPN using which you can connect to your VMware Software Defined Data Center (SDDC) vCenter and do any initial configuration required.

Before deploying a VPN gateway, configure the **Edge Services** range for the region where your SDDC is deployed. To do this:

1. Log on to the **Google Cloud VMware Engine** portal, and go to **Network > Regional Settings**. Click **Add Region**.
2. Choose the region where your SDDC is deployed and enable **Internet Access** and **Public IP Service**.
3. Supply the Edge Services range noted during planning and click **Submit**. Enabling these services take 10–15 minutes.

   Once complete, the Edge Services show as **Enabled** on the Regional Settings page. Enabling these settings allow Public IPs to be allocated to your SDDC, which is a requirement for deploying a VPN gateway.

Deploy a VPN gateway

1. In the **Google Cloud VMware Engine** portal, go to **Network > VPN Gateways**. Click **Create New VPN Gateway**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Supply the name for the VPN gateway and the client subnet reserved during planning. The location of the VPN must be the same as the private cloud region. Click **Next**.
3. Select users to grant VPN access. Click **Next**.
4. Specify the networks that must be accessible over VPN. Click **Next**.
5. A summary screen is displayed. Verify the selections, and click **Submit** to create the VPN Gateway. The VPN Gateways page is displayed with the status of the new VPN gateway as **Creating**.
6. After the status changes to **Operational**, click the new VPN gateway.
7. Click **Download my VPN configuration** to download a ZIP file containing pre-configured OpenVPN profiles for the VPN gateway. Profiles for connecting through UDP/1194 and TCP/443 are available. Choose your preference and import it into Open VPN, and then connect.
8. Go to **Resources** and select your SDDC.

CONNECT THE VPN

1. Establish a point-to-site connection between your on-premises network and the private cloud through the VPN Gateway setup. See Set up Google Cloud VMware Engine VPN Gateway.
2. Upload the VPN configuration downloaded in Set up Google Cloud VMware Engine VPN Gateway.
3. Import to your VPN client, for example, OpenVPN Connect.

For more information, see Connecting using VPN.

CREATE FIRST SUBNET

Access NSX-T Manager from the VMware Engine portal
The process of creating a subnet happens in NSX-T, which you access through VMware Engine. Do the following to access NSX-T Manager.

1. Log on to the **Google Cloud VMware Engine** portal.
2. From the main navigation, go to **Resources**.
3. Click the **Private cloud name** corresponding to the private cloud where you want to create the subnet.
4. On the details page of your private cloud, click the **vSphere Management Network** tab.
5. Click the **FQDN** corresponding to the NSX-T Manager.
6. When prompted, enter your sign-in credentials. If you have set up vIDM and connected it to an identity source, such as Active Directory, use your identity source credentials instead.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMINDER:

You can retrieve generated credentials from the private cloud details page.

Set up DHCP service for the subnet

Before you can create a subnet, set up a DHCP service:

In NSX-T Manager:

1. Go to **Networking > DHCP**. The networking dashboard shows that the DHCP service creates one Tier-0 and one Tier-1 gateway.
2. To begin provisioning a DHCP server, click **Add Server**.
3. Select **DHCP** for the **Server Type**, provide the server name and IP address.
4. Click **Save** to create the DHCP service.

Do the following to attach this DHCP service to the relevant Tier-1 gateway. A default Tier-1 gateway is already provisioned by the DHCP service:

1. Select **Tier 1 Gateways**, select the vertical ellipsis on the Tier-1 gateway, and then select **Edit**.
2. In the **IP Address Management** field, select **No IP Allocation Set**.
3. Select **DHCP Local Server** for the **Type**.
4. Select the DHCP server that you created for the **DHCP Server**.
5. Click **Save**.
6. Click **Close Editing**.

You can now create a network segment in NSX-T. For more information about DHCP in NSX-T, see the VMware documentation for DHCP.

Create a network segment in NSX-T

For workload VMs, you create subnets as NSX-T network segments for your private cloud:

1. In NSX-T Manager, go to **Networking > Segments**.
2. Click **Add Segment**.
3. Enter a name for the segment.
4. Select the **Tier-1** as the **Connected Gateway** and leave the Type as **Flexible**.
5. Click **Set Subnets**.
6. Click **Add Subnets**.

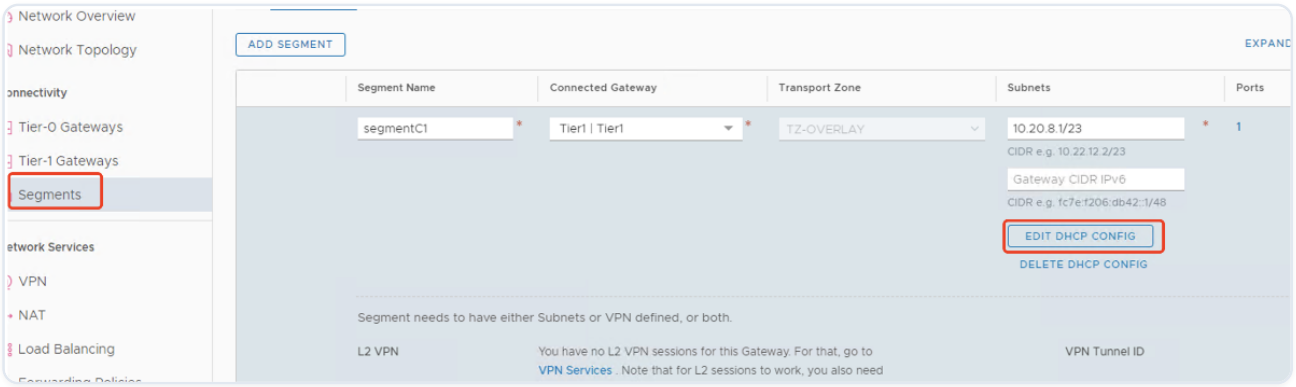
© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Enter the subnet range in the **Gateway IP/Prefix Length**. Specify the subnet range with **.1** as the last octet. For example, **10.12.2.1/24**.
8. Specify the DHCP Ranges and click **ADD**.
9. In **Transport Zone**, select **TZ-OVERLAY** from the drop-down list.
10. Click **Save**. You can now select this network segment in vCenter when creating a VM.

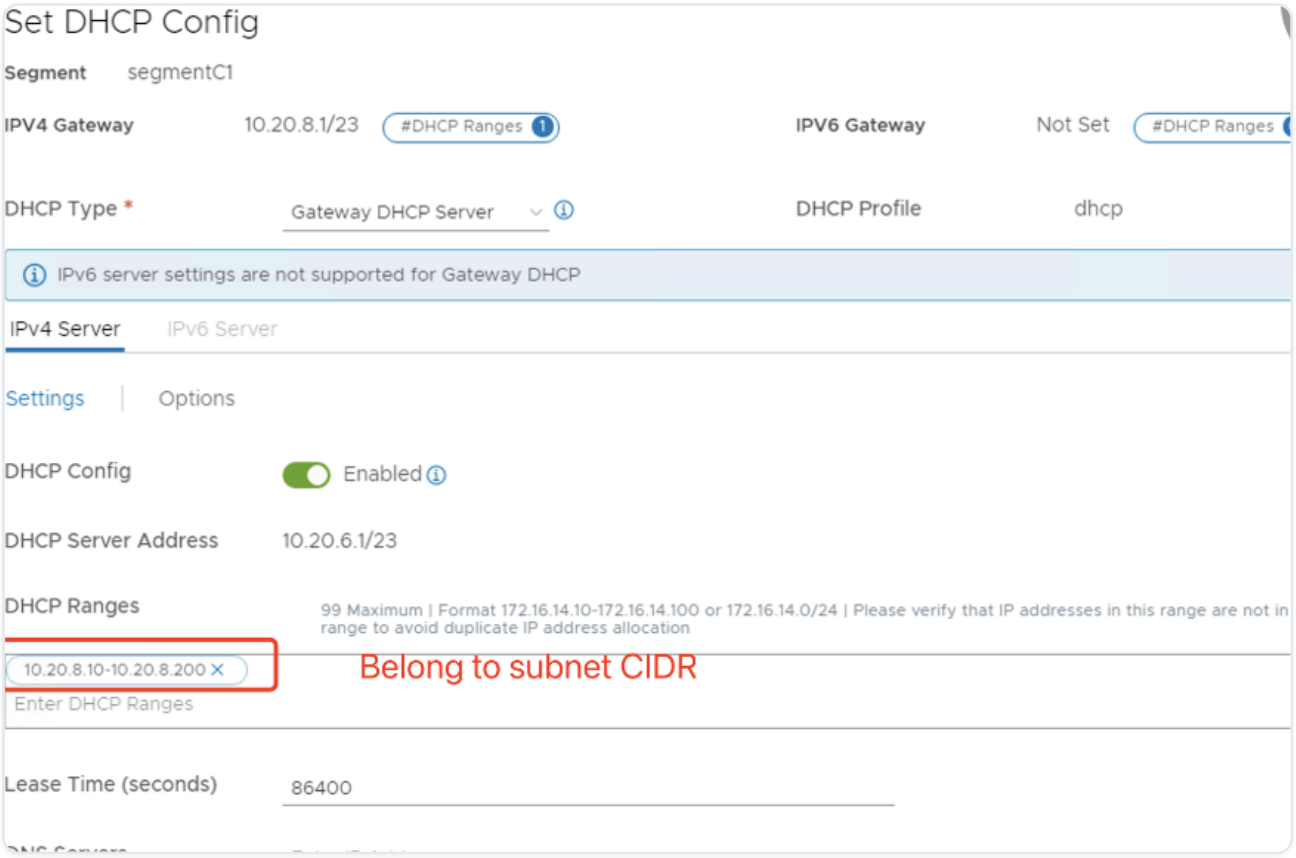
In a given region, you can set up at most 100 unique routes from VMware Engine to your VPC network using private services access. This includes, for example, private cloud management IP address ranges, NSX-T workload network segments, and HCX network IP address ranges. This limit includes all private clouds in the region.

NOTE:

There is a Google Cloud configuration issue because of which you need to configure DHCP range setting several times. Therefore, make sure to configure the DHCP range setting after Google Cloud configuration. Click **EDIT DHCP CONFIG** to configure the DHCP ranges.



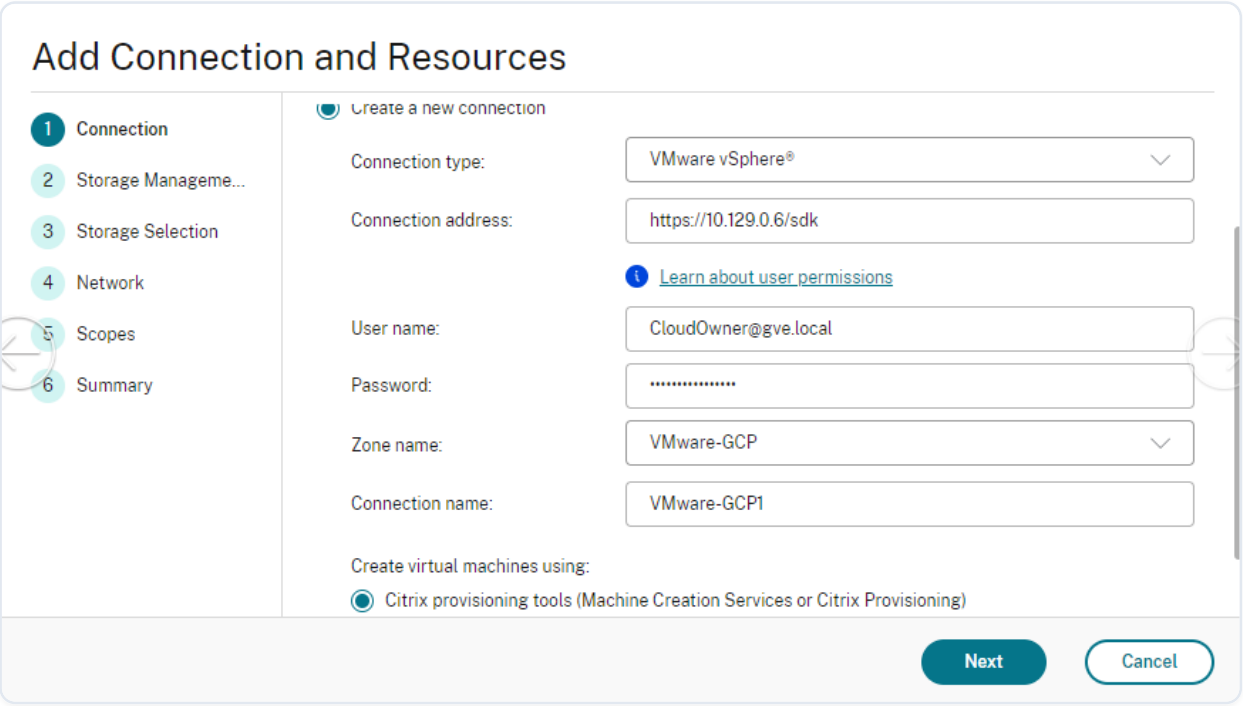
© 1997–2026 Citrix Systems, Inc. All rights reserved.



CREATE THE GOOGLE CLOUD VMWARE CONNECTION IN CITRIX STUDIO

1. Create a machine in vCenter and install a pair of Cloud Connectors in the machine. See Configure the instances.
2. Launch the Citrix Studio.
3. Select the hosting node, and click **Add Connection and Resources**.
4. On the **Connection** screen, select **Create a new Connection**, and the following details:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. Select **Connection type** as **VMware vSphere**.

b. In the **Connection address**, enter the vCenter private IP address.

c. Enter the vCenter credentials.

d. Enter a connection name.

e. Choose the tool to create virtual machines.

5. On the **Network** screen, select the subnet created in the NSX-T server.
6. Complete the wizard.

VMware cloud on Amazon Web Services (AWS)

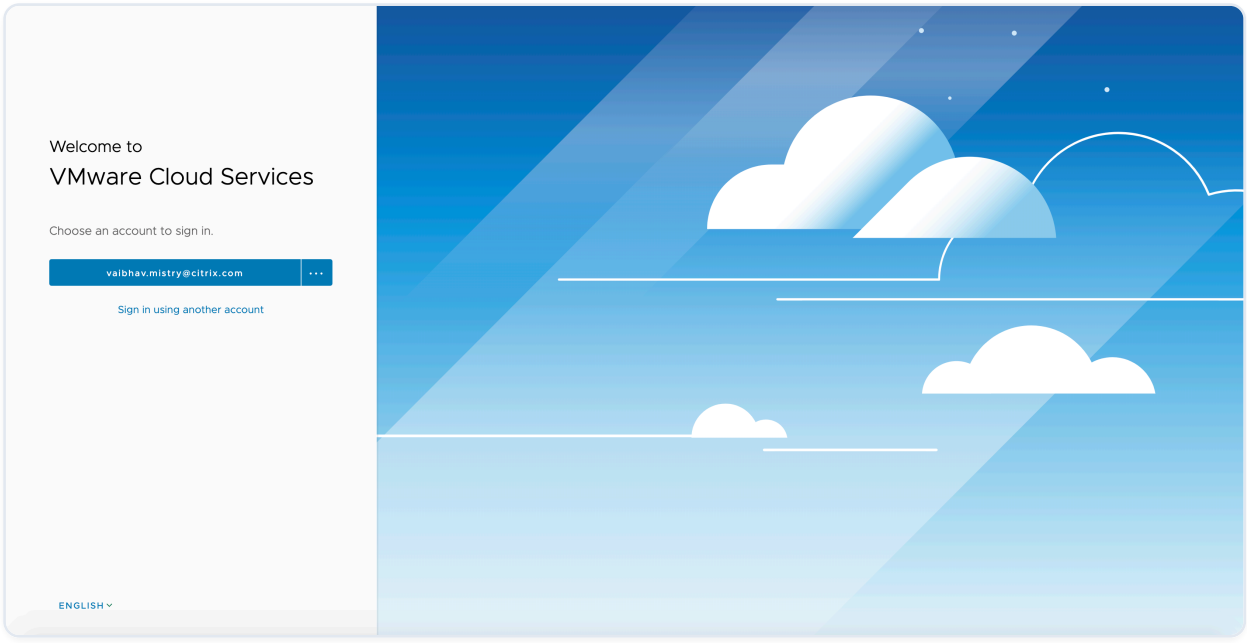
VMware cloud on Amazon Web Services (AWS) enables you to migrate VMware based on-premises Citrix workloads to AWS Cloud and your core Citrix Virtual Apps and Desktops environment to Citrix DaaS.

This article describes the procedure to set up a VMware cloud on AWS.

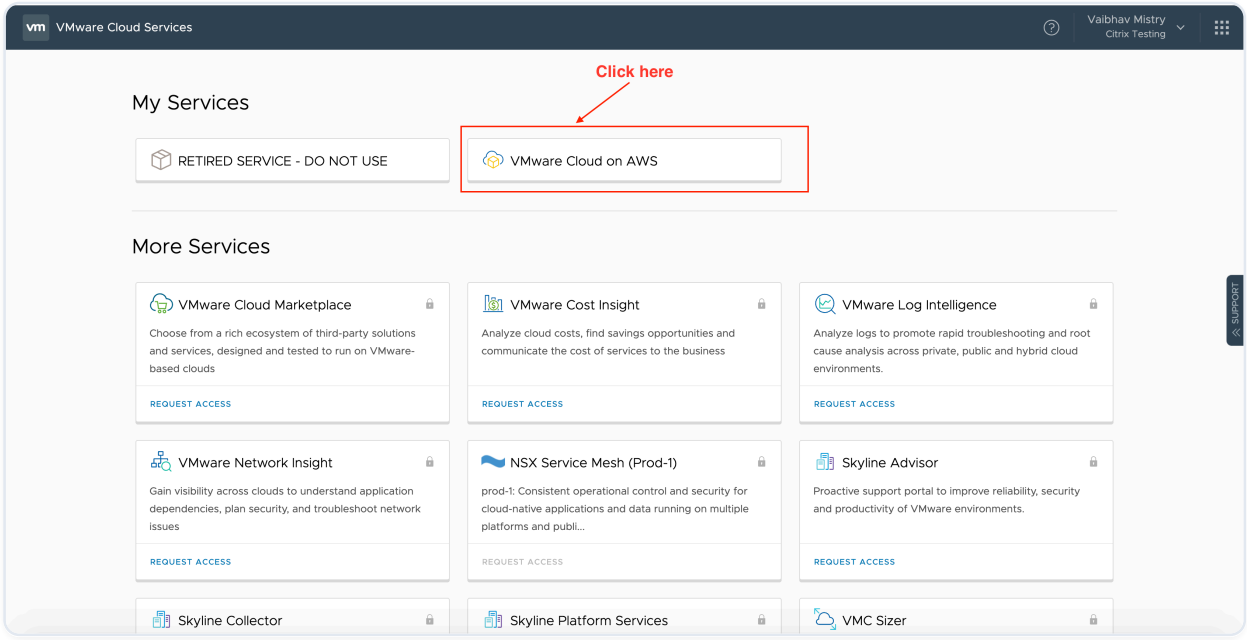
Access the VMware cloud environment

1. Log in to VMware cloud services using the URL `<https://console.cloud.vmware.com/>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

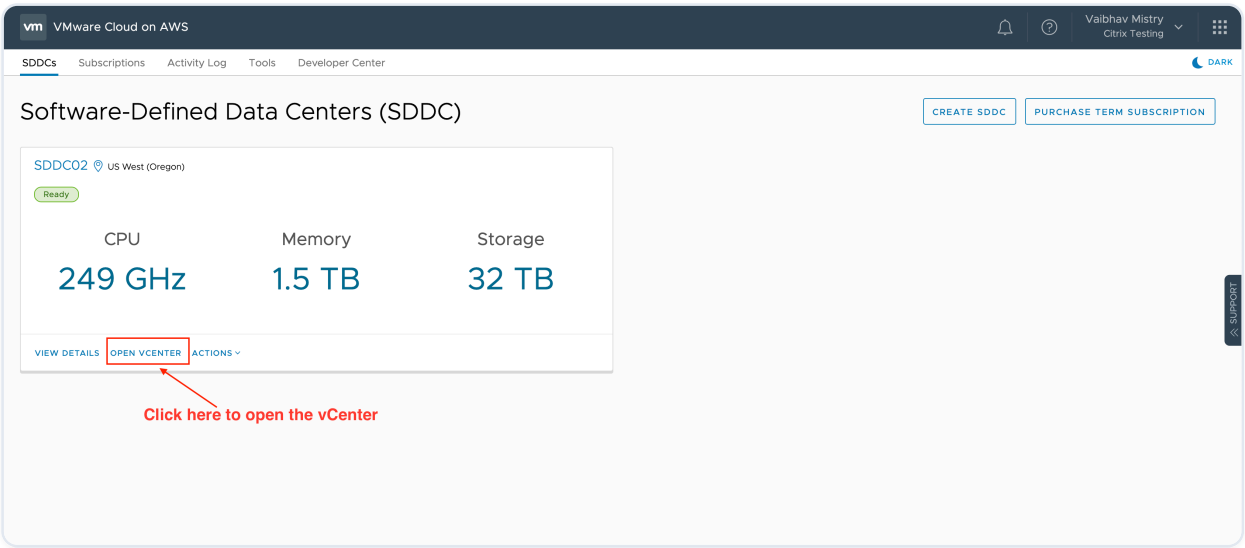


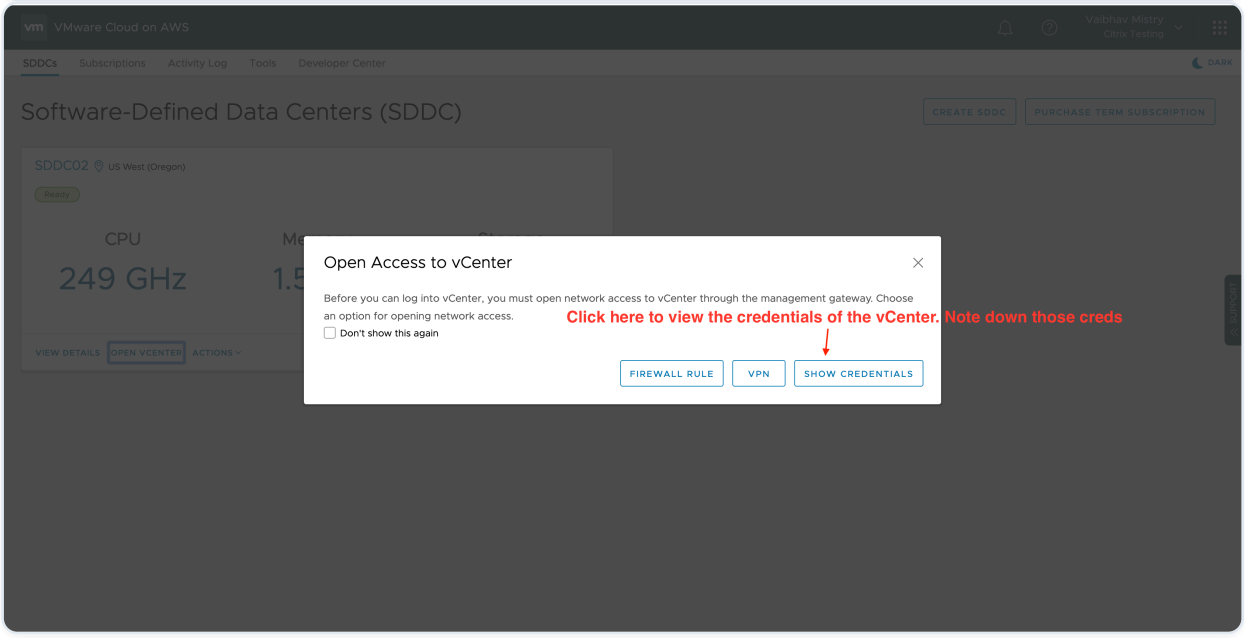
2. Click **VMware Cloud on AWS**. The page Software-Defined Data Centers (SDDC) appears.



3. Click **OPEN VCENTER**, and then click **SHOW CREDENTIALS**. Note the credentials for later use.

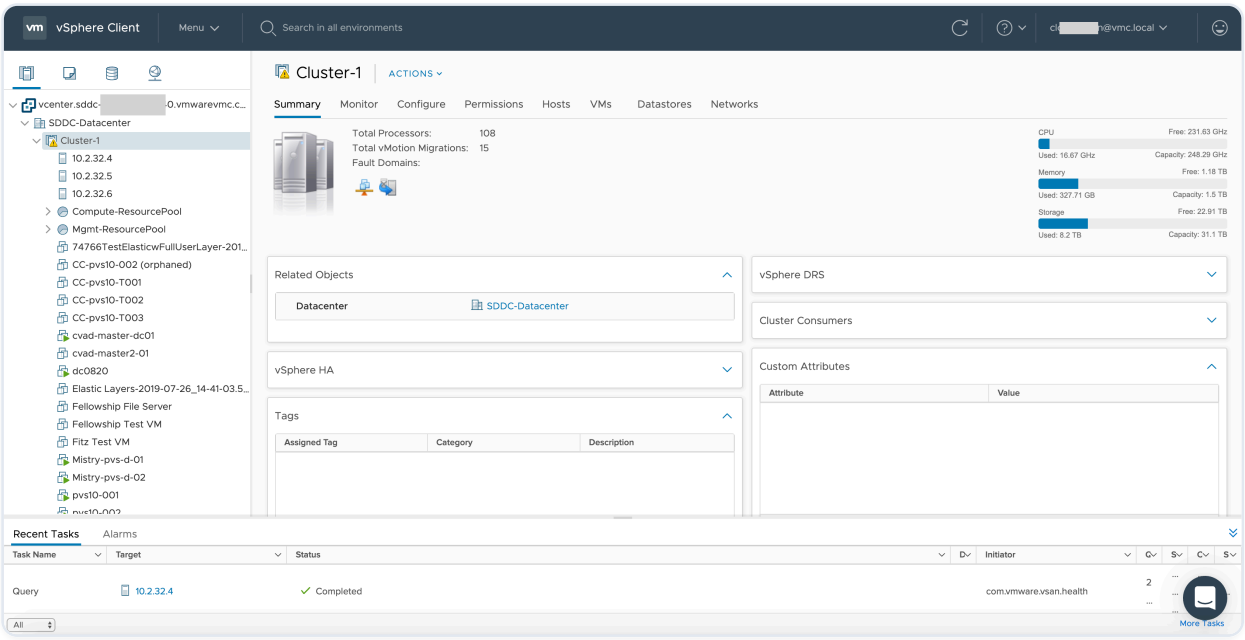
© 1997–2026 Citrix Systems, Inc. All rights reserved.





4. Open a Web browser and enter the URL for the vSphere Web Client.
5. Enter the credentials as noted and click **Login**. The vSphere client webpage is similar to the on-premises environment.

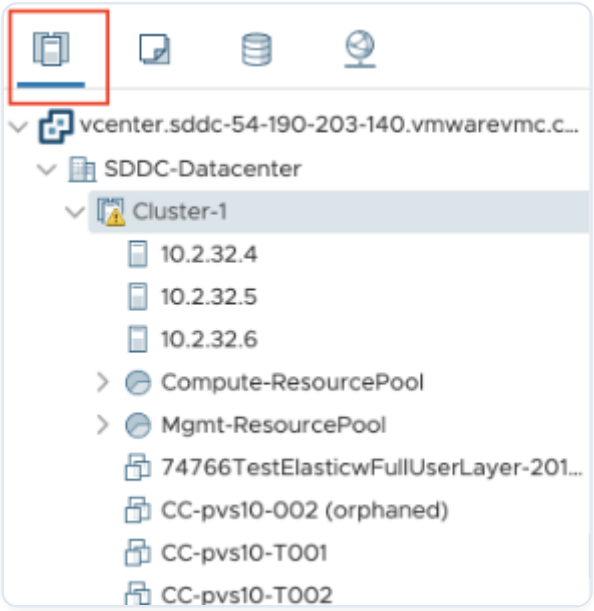
© 1997–2026 Citrix Systems, Inc. All rights reserved.



About VMware cloud environment

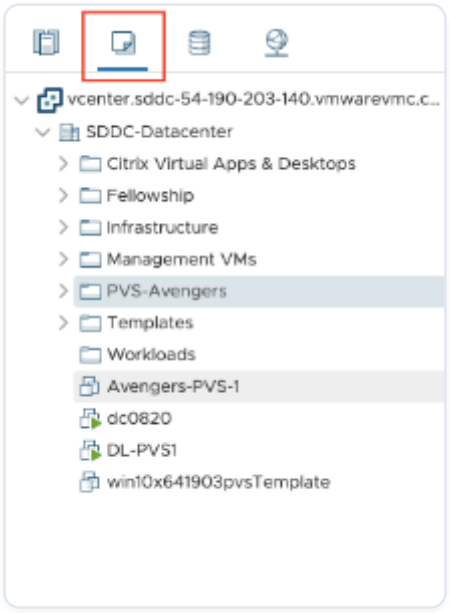
There are four views on the vSphere client webpage.

- Host and Cluster view: You cannot create a new Cluster, but the cloud admin can create multiple resource pools.

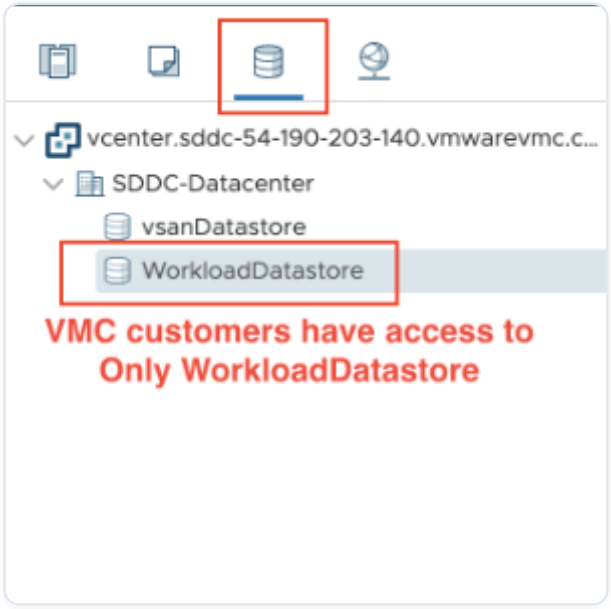


- VM and Template view: Cloud admin can create many folders.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

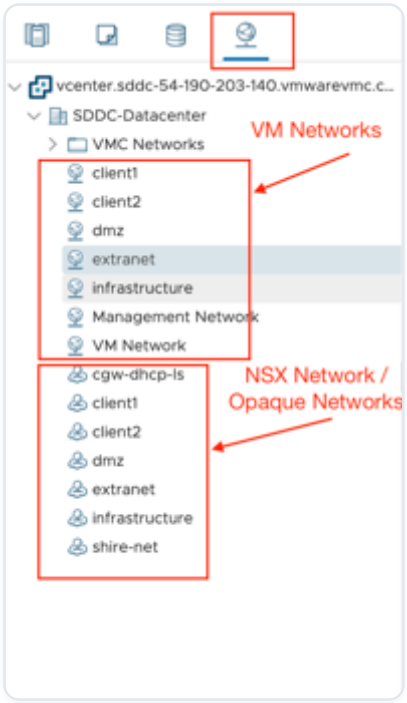


- Storage View: Select **WorkloadDatastore** storage when you add hosting unit in the Citrix Studio because you have access to only Workload Datastore.



- Network View: The icons are different for VMware cloud networks and opaque networks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After you set up the cluster, refer to VMware virtualization environments for adding connections and resources.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing a connection, see Connection to VMware cloud and partner solutions.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

XenServer® virtualization environments

XenServer simplifies your operational management while ensuring a high definition user experience for intensive workloads.

To set up your XenServer, see Add a resource type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine designated to deliver apps or a desktop to your users.
- For creating and managing connections, see Connection to XenServer.
- Review all the steps in the installation and configuration process.

More information

- Create and manage connections and resources
- Create machine catalogs

Size and scale considerations for Cloud Connectors

When evaluating Citrix DaaS for sizing and scalability, consider all the components. Research and test the configuration of Citrix Cloud™ Connectors and StoreFront for your specific requirements. Providing insufficient resources for sizing and scalability negatively affects the performance of your deployment.

NOTE:

- These recommendations apply to Citrix DaaS Standard for Azure in addition to Citrix DaaS.
- The tests and recommendations given in this article are guidelines to help you start your testing. We recommend that you perform the testing in your environment to validate the correct connector sizing.
- For sizing and scale considerations for HDX proxy, see Cloud Connector sizing and scale considerations for HDX proxy.

This article provides details of the tested maximum capacities and best practice recommendations for Cloud Connector machine configuration. Tests were performed on deployments configured with StoreFront™ and Local Host Cache (LHC).

The information provided applies to deployments in which each resource location contains both VDI workloads and RDS workloads.

The Cloud Connector links your workloads to Citrix DaaS™ in the following ways:

- Provides a proxy for communication between your VDAs and Citrix DaaS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Provides a proxy for communication between Citrix DaaS and your Active Directory (AD) and hypervisors.
- In deployments that include StoreFront servers, the Cloud Connector serves as a temporary session broker during cloud outages, providing users with continued access to resources.

It is important to have your Cloud Connectors properly sized and configured to meet your specific needs. While tests were run with two Cloud Connectors, only one Cloud Connector is available during Cloud Connector upgrades. To ensure high availability during Cloud Connector upgrades, some customers have opted to deploy three Cloud Connectors.

Each set of Cloud Connectors is assigned to a resource location (also known as a zone in Studio). A resource location is a logical separation that specifies which resources communicate with that set of Cloud Connectors. At least one resource location is required per domain to communicate with the Active Directory (AD).

Each machine catalog and hosting connection is assigned to a resource location.

For deployments with more than one resource location, assign machine catalogs and VDAs to the resource locations to optimize the ability of LHC to broker connections during outages. For more information on creating and managing resource locations, see Connect to Citrix Cloud. For optimum performance, configure your Cloud Connectors on low-latency connections to VDAs, AD servers, and hypervisors.

Recommended processors and storage

For performance similar to that seen in these tests, use modern processors that support SHA extensions. SHA extensions reduce the cryptographic load on the CPU. Recommended processors include:

- Advanced Micro Devices (AMD) Zen and newer processors
- Intel Ice Lake and newer processors

The recommended processors run efficiently. You can use older processors, however, it might lead to a higher CPU load. We recommend increasing your vCPU count to offset this behavior.

The tests described in this article were performed with AMD EPYC and Intel Cascade Lake processors.

Cloud Connectors have a heavy cryptographic load while communicating with the cloud. Cloud Connectors using processors with SHA extensions experience lower load on their CPU which is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

expressed by lower CPU usage by the Windows Local Security Authority Subsystem Service (LSASS).

Citrix recommends using modern storage with adequate I/O operations per second (IOPS), especially for deployments that use LHC. Solid state drives (SSDs) are suggested but premium cloud storage tiers are not needed. Higher IOPS are needed for LHC scenarios where the Cloud Connector runs a small copy of the database. This database is updated with site configuration changes regularly and provides brokering capabilities to the resource location in times of Citrix Cloud outages.

Recommended compute configuration for Local Host Cache

Local Host Cache (LHC) provides high availability by enabling connection brokering operations in a deployment to continue when a Cloud Connector cannot communicate with Citrix Cloud.

Cloud Connectors run Microsoft SQL Express Server LocalDB, which is automatically installed when you install the Cloud Connector. The CPU configuration of the Cloud Connector, especially the number of cores available to SQL Express Server LocalDB, directly affects LHC performance. The number of CPU cores available to SQL Server Express Server LocalDB affects LHC performance even more than memory allocation does. This CPU overhead is observed only when in LHC mode when Citrix DaaS is not reachable, and the LHC broker is active. For any deployment using LHC, Citrix recommends four cores per socket, with a minimum of four CPU cores per Cloud Connector. For information on configuring compute resources for SQL Express Server LocalDB, see Compute capacity limits by edition of SQL Server.

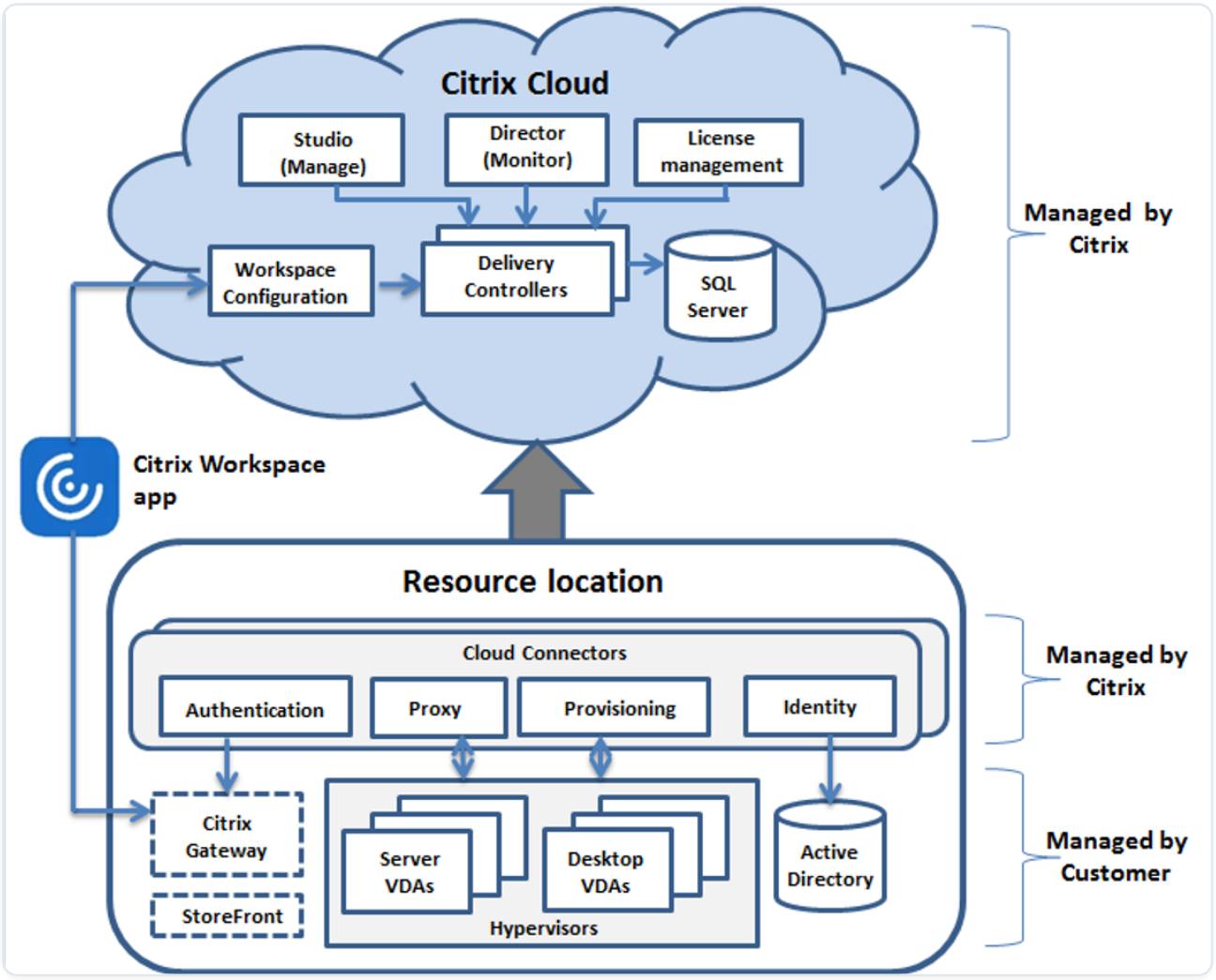
If compute resources available to the SQL Express Server LocalDB are misconfigured, configuration synchronization times might be increased and performance during outages might be reduced. In some virtualized environments, compute capacity might depend on the number of logical processors and not CPU cores.

Summary of test findings

All results in this summary are based on the findings from a test environment as configured in the detailed sections of this article. The results shown here are for a single resource location. Different system configurations might yield different results.

This illustration gives a graphical overview of the tested configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following table shows the minimum recommended Cloud Connector CPU and memory configurations for sites of various sizes. Results of testing with these configurations are shown below. See Limits for more information on the resource location limits.

	MEDIUM	LARGE	MAXIMUM
Connectors for HA	2	2	3
VDAs	Up to 1000	1001 - 5000	5001 - 10,000
Sessions	Up to 2500	Up to 10,000	Up to 25,000
Hosting connections	Up to 20	Up to 40	Up to 40
CPUs for Cloud Connectors	4vCPU	4vCPU	8vCPU
Memory for Cloud Connectors	6 GB	8 GB	10 GB

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If your deployment exceeds 5000 VDAs, you must use three Cloud Connectors for high availability and scalability.

Test methodology

Tests were conducted to add load and to measure the performance of the environment components. The components were monitored by collecting performance data and procedure timing, such as logon time and registration time. Sometimes, proprietary Citrix simulation tools are used to simulate VDAs and sessions. These tools are designed to exercise Citrix components the same way that traditional VDAs and sessions do, without the same resource requirements to host real sessions and VDAs. Tests were conducted in both cloud brokering and LHC mode for scenarios with Citrix StoreFront.

Recommendations for Cloud Connector sizing in this article are based on data gathered from these tests.

The following tests were run:

- **Session logon/launch storm:** a test that simulates high-volume logon periods.
- **VDA registration storm:** a test that simulates high-volume VDA registration periods. For example, following an upgrade cycle or transitioning between cloud brokering and Local Host Cache mode.
- **VDA power action storm:** a test that simulates high-volume of VDA power actions.

Test scenarios and conditions

These tests were performed with LHC configured. For more information about using LHC, see the Local Host Cache article. LHC requires an on-premises StoreFront server. For detailed information about StoreFront, see the StoreFront product documentation.

Recommendations for StoreFront configurations:

- If you have multiple resource locations with a single StoreFront server or server group, enable the advanced health check option for the StoreFront store. See StoreFront requirement in the Local Host Cache article.
- For higher session launch rates, use a StoreFront server group. See Configure server groups in the StoreFront product documentation.

Test conditions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CPU and memory requirements are for the base OS and Citrix services only. Third-party apps and services might require additional resources.
- VDAs are any virtual or physical machines running Citrix Virtual Delivery Agent.
- Tests are performed using Windows VDAs only.
- All VDAs tested were power-managed using Citrix DaaS.
- Session were launched at a sustained rate of 1,000 per minute.
- Workloads of 1,000 to 10,000 VDI and 500–10,000 RDS servers with 1,000-25,000 sessions were tested.
- RDS sessions were tested up to 25,000 per resource location.
- Tests were performed using two Cloud Connectors in both normal operations and during outage. Citrix recommends using at least two Cloud Connectors for high availability, and three Cloud Connectors for maximum and large sized resource locations. When in outage mode, only one of the Cloud Connectors is used for VDA registrations and brokering. While tests were run with two Cloud Connectors, only one Cloud Connector is available during upgrades. To ensure high availability during upgrades, some customers have opted to run with three Cloud Connectors.
- Tests were performed with the Cloud Connector configured with Intel Cascade Lake processors.
- Sessions were launched via a single Citrix StoreFront server.
- LHC outage sessions launch tests conducted after machines had re-registered.

RDS session counts are a recommendation and not a limit. Test your own RDS session limit in your environment.

NOTE:

Session count and launch rate are more important for RDS than the VDA count.

Medium workloads

These workloads were tested with 4 vCPUs and 6 GB memory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TEST WORKLOADS	SITE CONDITION	VDA REGISTRATION TIME	REGISTRATION CPU AND MEMORY USAGE	LAUNCH TEST LENGTH	SESSION LAUNCH CPU AND MEMORY USAGE	LAUNCH RATE
1000 VDI	Online	5 minutes	CPU maximum = 36%, CPU average = 33%, memory maximum = 5.3 GB	2 minutes	CPU maximum = 29%, CPU average = 27%, memory maximum = 3.7 GB	500 per minute
1000 VDI	Outage	4 minutes	CPU maximum = 11%, CPU average = 10%, memory maximum = 4.5 GB	2 minutes	CPU maximum = 42%, CPU average = 28%, memory maximum = 4.0 GB	500 per minute
250 RDS, 5000 sessions	Online	3 minutes	CPU maximum = 14%, CPU average = 4%, memory maximum = 3.5 GB	9 minutes	CPU maximum = 46%, CPU average = 21%, memory maximum = 3.7 GB	555 per minute
250 RDS, 5000 sessions	Outage	3 minutes	CPU maximum = 15%, CPU average = 5%, memory	9 minutes	CPU maximum = 51%, CPU average = 32%, memory	555 per minute

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TEST WORKLOADS	SITE CONDITION	VDA REGISTRATION TIME	REGISTRATION CPU AND MEMORY USAGE	LAUNCH TEST LENGTH	SESSION LAUNCH CPU AND MEMORY USAGE	LAUNCH RATE
			maximum = 3.7		maximum = 4.2 GB	

Large workloads

These workloads were tested with 4 vCPUs and 8 GB memory.

TEST WORKLOADS	SITE CONDITION	VDA REGISTRATION TIME	REGISTRATION CPU AND MEMORY USAGE	LAUNCH TEST LENGTH	SESSION LAUNCH CPU AND MEMORY USAGE	LAUNCH RATE
5000 VDI	Online	3–4 minutes	CPU maximum = 45%, CPU average = 25%, memory maximum = 7.0 GB	5 minutes	CPU maximum = 75%, CPU average = 55%, memory maximum = 7.0 GB	1000 per minute
5000 VDI	Outage	4–6 minutes	CPU maximum = 15%, CPU average = 5%, memory maximum = 7.5 GB	5 minutes	CPU maximum = 45%, CPU average = 40%, memory maximum = 7.5 GB	1000 per minute
500 RDS, 10,000 sessions	Online	3 minutes	CPU maximum = 45%, CPU average =	10 minutes	CPU maximum = 75%, CPU average =	1000 per minute

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TEST WORKLOADS	SITE CONDITION	VDA REGISTRATION TIME	REGISTRATION CPU AND MEMORY USAGE	LAUNCH TEST LENGTH	SESSION LAUNCH CPU AND MEMORY USAGE	LAUNCH RATE
			25%, memory maximum = 7.0 GB		55%, memory maximum = 7.0 GB	
500 RDS, 10,000 sessions	Outage	3 minutes	CPU maximum = 15%, CPU average = 5%, memory maximum = 7.5	10 minutes	CPU maximum = 45%, CPU average = 40%, memory maximum = 7.5 GB	1000 per minute

Maximum workloads

These workloads were tested with 8 vCPUs and 10 GB memory.

TEST WORKLOADS	SITE CONDITION	VDA REGISTRATION TIME	REGISTRATION CPU AND MEMORY USAGE	LAUNCH TEST LENGTH	SESSION LAUNCH CPU AND MEMORY USAGE	LAUNCH RATE
10,000 VDI	Online	3–4 minutes	CPU maximum = 85%, CPU average = 10%, memory maximum = 8.5 GB	7 minutes	CPU maximum = 66%, CPU average = 28%, memory maximum = 7.0 GB	1400 per minute
10,000 VDI	Outage	4–5 minutes	CPU maximum = 90%,	5 minutes	CPU maximum = 90%,	2000 per minute

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TEST WORKLOADS	SITE CONDITION	VDA REGISTRATION TIME	REGISTRATION CPU AND MEMORY USAGE	LAUNCH TEST LENGTH	SESSION LAUNCH CPU AND MEMORY USAGE	LAUNCH RATE
			CPU average = 17%, memory maximum = 8.2 GB		CPU average = 45%, memory maximum = 8.5 GB	
1000 RDS, 20,000 sessions	Online	1–2 minutes	CPU maximum = 60%, CPU average = 20%, memory maximum = 8.6 GB	17 minutes	CPU maximum = 66%, CPU average = 25%, memory maximum = 6.8 GB	1200 per minute
1000 RDS, 20,000 sessions	Outage	3–4 minutes	CPU maximum = 22%, CPU average = 10%, memory maximum = 8.5	21 minutes	CPU maximum = 90%, CPU average = 50%, memory maximum = 7.5 GB	1000 per minute

NOTE:

The workloads shown here are the maximum recommended workloads for one resource location. To support larger workloads, add more resource locations.

Configuration synchronization resource usages

The configuration synchronization process keeps the Cloud Connectors up to date with Citrix DaaS. Updates are automatically sent to the Cloud Connectors to make sure that the Cloud Connectors are ready to take over brokering if an outage occurs. The configuration synchronization

© 1997–2026 Citrix Systems, Inc. All rights reserved.

updates the LHC database, SQL Express Server LocalDB. The process imports the data to a temporary database then switches to that database once imported. This ensures that there is always an LHC database ready to take over.

The CPU, memory, and disk usage are temporarily increased while data is imported to the temporary database.

Test conditions:

- Tested on an 8 vCPU AMD EPYC
- The imported site configuration database was for an environment with site-wide total of 80,000 VDAs and 300,000 users (three shifts of 100,000 users)
- Data import time was tested on a resource location with 10,000 VDI

Test results:

- **Data import time:** 7–10 minutes
- **CPU usage:**
  - maximum = 25%
  - average = 15%
- **Memory usage:**
  - increase of approximately 2 GB to 3 GB
- **Disk usage:**
  - 4 MB/s disk read spike
  - 18 MB/s disk write spike
  - 70 MB/s disk write spike during downloading and writing of xml config files
  - 4 MB/s disk read spike at the completion of import
- **LHC database size:**
  - 400–500 MB database file
  - 200–300 MB log database

Additional resource usage considerations:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- During import the full site configuration data is downloaded. This download might cause a memory spike, depending on the site size. If memory spikes are occurring during configuration syncs, consider increasing the size of the Cloud Connectors.
- The tested site used approximately 800 MB for the database and database log files combined. During a configuration synchronization, these files are duplicated with a maximum combined size of approximately 1600 MB. Ensure that your Cloud Connector has enough disk space for the duplicated files. The configuration synchronization process fails if the disk is full.

Install VDAs

Introduction

This article begins with a description of Windows VDAs and the available VDA installers. The remainder of the article describes the steps in the VDA installation wizard. Command-line equivalents are provided. For details, see Install VDAs using the command line.

For information about Linux VDAs, see Linux Virtual Delivery Agent.

View an introduction to VDAs.



Installation considerations

The Citrix DaaS article describes what VDAs are and what they do. Here's more information.

- **Analytics collection:** Analytics are collected automatically when you install or upgrade components. By default, that data is uploaded to Citrix automatically when the installation completes. Also, when you install components, you are automatically enrolled in the Citrix Customer Experience Improvement Program (CEIP), which uploads anonymous data. Also, during an installation or upgrade, you're offered the opportunity to enroll in Call Home.

  If a VDA installation fails, an MSI analyzer parses the failing MSI log, displaying the exact error code. The analyzer suggests a CTX article, if it is a known issue. The analyzer also collects anonymized data about the failure error code. This data is included with other data collected by CEIP. If you end enrollment in CEIP, the collected MSI analyzer data is no longer sent to Citrix.

  For information about these programs, see Citrix Insight Services.
- **Citrix Workspace™ app:** Citrix Workspace app for Windows is not installed by default when you install a VDA. You can download and install or upgrade Citrix Workspace app for Windows

© 1997–2026 Citrix Systems, Inc. All rights reserved.

and other Citrix Workspace apps from the Citrix website. Alternatively, you can make those Citrix Workspace apps available from the Workspace or a StoreFront™ server.

- **Print Spooler Service:** The Microsoft Print Spooler Service must be enabled. You cannot successfully install a VDA if that service is disabled.
- **Microsoft Media Foundation:** Most supported Windows editions come with Media Foundation already installed. If the machine on which you're installing a VDA does not have Microsoft Media Foundation (such as N editions), several multimedia features are not installed and do not work.
  - Flash Redirection
  - Windows Media Redirection
  - HTML5 Video Redirection
  - HDX™ RealTime Webcam Redirection

  You can acknowledge the limitation, or end the VDA installation and restart it later, after installing Media Foundation. In the graphical interface, this choice is presented in a message. In the command line, you can use the `/no_mediafoundation_ack` option to acknowledge the limitation.
- **Local user group:** When you install the VDA, a new local user group called Direct Access Users is created automatically. For a single-session OS VDA, this group applies only to RDP connections. For a multi-session OS VDA, this group applies to ICA® and RDP connections.
- **Cloud Connector address requirement:** The VDA must have at least one valid Cloud Connector address (in the same resource location) with which to communicate. Otherwise, sessions cannot be established. You specify Cloud Connector addresses when you install the VDA. For information about other ways to specify Cloud Connector addresses where VDAs can register, see VDA registration.
- **Operating system considerations:**
  - Review the System requirements for supported platforms, operating systems, and versions.
  - Ensure that each operating system maintains the latest updates.
  - Ensure that VDAs have synchronized system clocks. The Kerberos infrastructure that secures communication between the machines requires synchronization.
  - Optimization guidance for Windows 10 machines is available in CTX216252.
  - If you try to install (or upgrade to) a Windows VDA on an OS that is not supported for that VDA version, a message describes your options. For more information, see System requirements and Earlier operating systems.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Installed MSIs:** Several MSIs are installed automatically when you install a VDA. You can prevent the installation of some MSIs on the **Additional Components** page of the graphical interface or with the `/exclude` option in the CLI. For others, the only way to prevent their installation is with the `/exclude` CLI option.
- **Domain-joined:** Ensure that the machine is domain-joined before installing the VDA software.

Restarts during VDA installation

A restart is required at the end of the VDA installation. That restart occurs automatically by default.

To minimize the number of other restarts needed during VDA installation:

- Ensure that a supported Microsoft .NET Framework version is installed before beginning the VDA installation.
- For Windows multi-session OS machines, install and enable the RDS role services before installing the VDA.

If you do not install those prerequisites before installing the VDA:

- If you are using the graphical interface or the command line interface without the `/noreboot` option, the machine restarts automatically after installing the prerequisite.
- If you are using the command line interface with the `/noreboot` option, you must initiate the restart.

After each restart, the VDA installation continues. If you're installing from the command line, you can prevent the automatic resumption with the `/noresume` option.

When upgrading a VDA to version 7.17 or a later supported version, a restart occurs during the upgrade. This restart cannot be avoided.

Restore on install or upgrade failure

NOTE:

This feature is available only for single-session VDAs.

If a single-session VDA installation or upgrade fails, and the "restore on failure" feature is enabled, the machine is returned to a restore point that was set before the installation or upgrade began.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When a single-session VDA installation or upgrade starts with this feature enabled, the installer creates a system restore point before beginning the actual install or upgrade. If the VDA installation or upgrade fails, the machine is returned to the restore point state. The `%temp%/Citrix` folder contains deployment logs and other information about the restore.

By default, this feature is disabled.

If you plan to enable this feature, make sure that system restore is not disabled through a GPO setting (`Computer Configuration > Administrative Templates > System > System Restore`).

To enable this feature when installing or upgrading a single-session VDA:

- When using a VDA installer's graphical interface (such as using **Autostart** or the `XenDesktopVDASetup.exe` command without any restore or quiet options), select the **Enable automatic restore if update fails** check box on the **Summary** page.

  If the install/upgrade completes successfully, the restore point is not used, but is retained.
- Run a VDA installer with either the `/enablerestore` or `/enablerestorecleanup` option.
  - If you use the `/enablerestorecleanup` option, and the install/upgrade completes successfully, the restore point is removed automatically.
  - If you use the `/enablerestore` option, and the install/upgrade completes successfully, the restore point is not used, but is retained.

VDA installers

VDA installers can be downloaded directly from the Citrix Cloud™ console.

By default, files in the self-extracting installers are extracted to the `Temp` folder. The files extracted to the `Temp` folder are automatically deleted after the installation completes. Alternatively, you can use the `/extract` command with an absolute path.

Three standalone VDA installers are available for download.

VDAServerSetup.exe Installs a multi-session OS VDA.

VDAWorkstationSetup.exe Installs a single-session OS VDA.

VDAWorkstationCoreSetup.exe Installs a single-session OS VDA that is optimized for Remote PC Access deployments or core VDI installations. Remote PC Access uses physical machines. Core VDI installations are VMs that are not being used as an image. This installer deploys only the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

core services necessary for VDA connections. Therefore, it supports only a subset of the options that are valid with the VDAWorkstationSetup installer.

For more information, see Install VDA for your respective versions.

Troubleshoot

In the Studio display for a delivery group, the **Installed VDA version** entry on the Details pane mightn't be the version installed on the machines. The machine's Windows Programs and Features display shows the actual VDA version.

Citrix Optimizer

Citrix Optimizer is a tool for Windows OS that helps Citrix administrators optimize VDAs by removing and optimizing various components.

After installing a VDA and completing the final restart, download and install Citrix Optimizer. See CTX224676. The CTX article contains the download package, plus instructions about installing and using Citrix Optimizer.

Customize a VDA

Later, to customize (change information for) an installed VDA:

1. From the Windows feature for removing or changing programs, select **Citrix Virtual Delivery Agent** or **Citrix Remote PC Access/VDI Core Services VDA**. Then right-click and select **Change**.
2. Select **Customize Virtual Delivery Agent Settings**.

When the installer launches, change any available settings.

Customize the port for communicating with Cloud Connectors

You can customize the port that VDAs use to communicate with Cloud Connectors based on your specific security requirements. This feature is useful if your security team doesn't allow the default port (port 80) to be open or if the default port is already in use.

NOTE:

When changing the default port number, only values within the range 1024–65535 are supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To customize the port, complete the following steps:

1. Add the VDA port number on Citrix Cloud Connectors
2. Additional Citrix Cloud Connector™ configuration when using Rendezvous V1
3. Add the VDA port number on VDAs

Add the VDA port number on Citrix Cloud Connectors

Go to the Citrix Cloud Connector and run the following two PowerShell commands:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe' -VdaPort <port number>`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe' -VdaPort <port number> -ConfigureFirewall`

Example:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe' -VdaPort 18000`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe' -VdaPort 18000 -ConfigureFirewall`

When customizing the port, consider the following:

- You must use the same port number in both commands.
- You must run both commands *on all Cloud Connectors*.
- To successfully communicate with Cloud Connectors, ensure that all VDAs use the same port number.
- The port you configure persists across connector updates.

Additional Citrix Cloud Connector configuration when using Rendezvous V1

Set the following registry key on each Citrix Cloud Connector:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist`

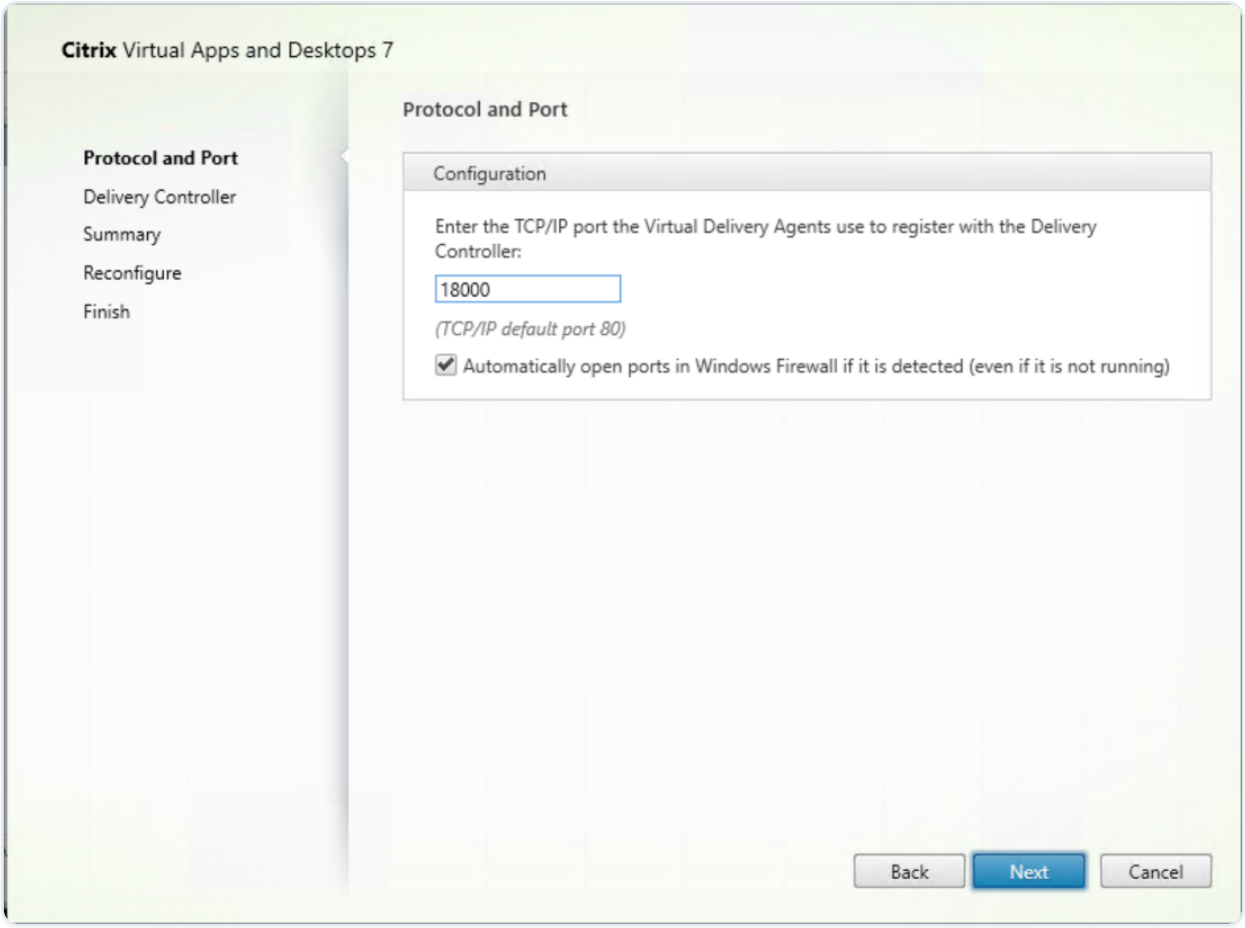
Name: `WorkerPortNumber` Type: `REG_DWORD` Value: `<port number>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add the VDA port number on VDAs

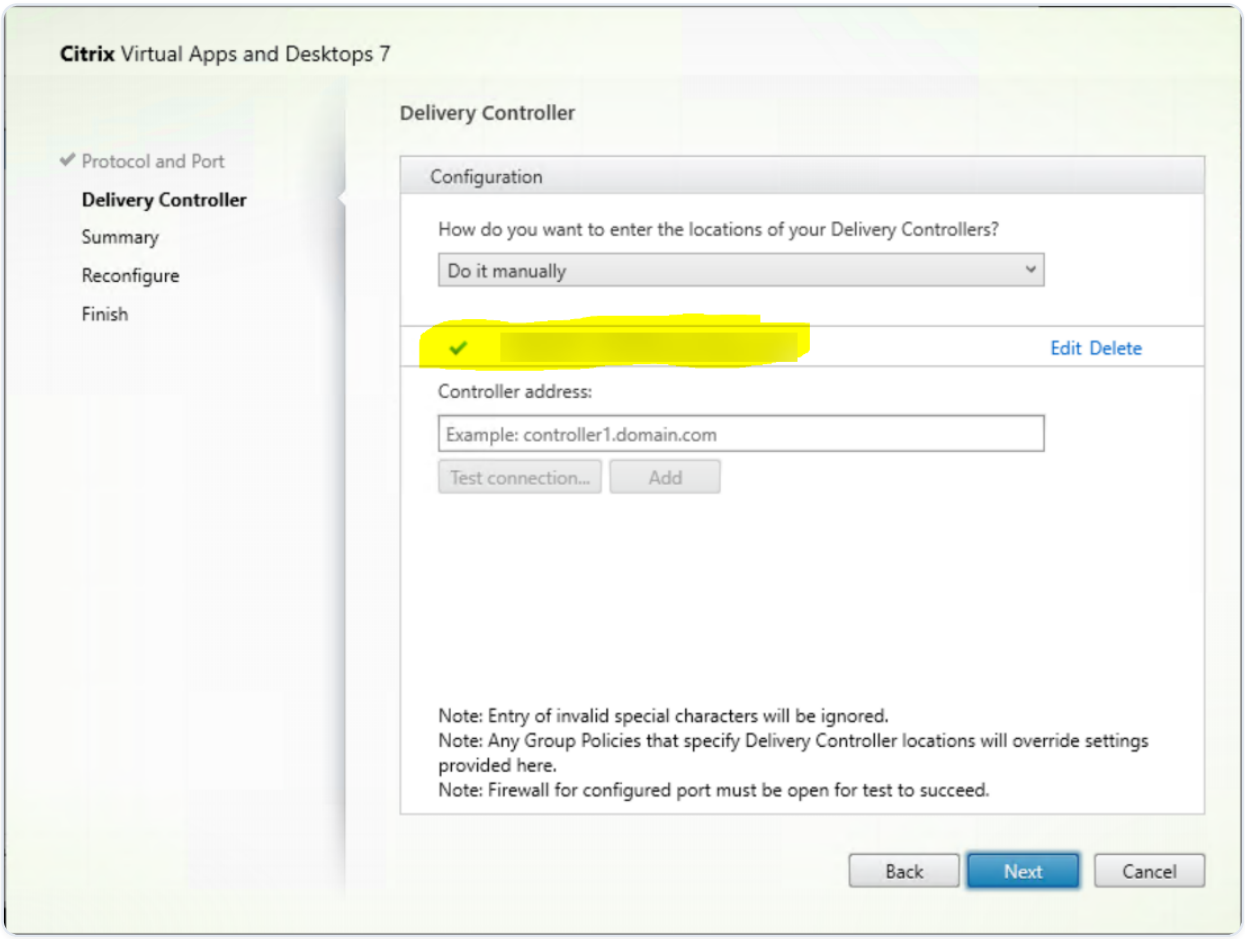
Install the VDA with default settings and configure as follows. If the VDA is already installed, continue with the steps below.

1. On the VDA, open **XenDesktopVdaSetup.exe**, which is located at `C:\Program Files\Citrix\XenDesktopVdaSetup\XenDesktopVdaSetup.exe`.
2. On the **Protocol and Port** page, add the custom port number.



3. On the **Delivery Controller™** page, enter the FQDN of the Controller.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click **Next** to proceed through the wizard to complete the configuration.

The port numbers are then reconfigured successfully.

NOTE:

You might see the following error message when you test a Controller connection: No running instance of a Controller found on < the Controller address you entered >. If the address is correct, you can dismiss the message.

Troubleshooting

To check whether the custom ports are configured correctly, go to the Cloud Connector and perform the following troubleshooting steps:

1. Verify that the following two registry keys exist.

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist Name: CustomVDAPortNumber Type: REG_DWORD Data: 18000

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist Name: CustomVDAPortNumberHA Type: REG_DWORD Data: 18000

2. Run the following command to create a .txt file.

   - `netsh http show urlacl > <filepath>.txt`

   Example:

   - `netsh http show urlacl > c:\reservations.txt`

3. Open the .txt file and check the following four URLs to verify that the correct port is used.

   - `http://+:18000/Citrix/CdsController/IRegistrar/`
   - `http://+:18000/Citrix/CdsController/ITicketing/`
   - `http://+:18000/Citrix/CdsController/IDynamicDataSink/`
   - `http://+:18000/Citrix/CdsController/INotifyBroker/`

4. Verify that the following two firewall rules are created and required ports are open.

   - Citrix XaXdProxy
   - Citrix Broker Service (TCP-In)

Other information

- After you install a VDA, you can check the health and availability of the site and its components with a Cloud Health check.

Where to go next

Create machine catalogs.

To review the entire configuration process, see Plan and build a deployment.

Install VDAs using the command line

Introduction

This article applies to installing, upgrading, and customizing Virtual Delivery Agents (VDAs) on machines with Windows operating systems.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This article describes how to issue VDA installation commands. Before beginning an installation, review Install VDAs to learn about installation considerations, installers, and what you specify during installation.

Install a VDA from the command line

To install a VDA (and see command execution progress and return values), you must have elevated administrative permissions or use **Run as administrator**.

1. On the machine where you're installing the VDA, sign to Citrix Cloud.
2. In the upper left menu, select **Solutions > DaaS**.
3. On the upper right side, click **Downloads** and select **Download VDA**. You're redirected to the VDA download page. Find the VDA installer that you want and click **Download File**.
4. After the download completes, run its name. Use the options described in this article.
    - For the multi-session OS Virtual Delivery Agent, run `VDAServerSetup.exe`
    - For the single-session OS Virtual Delivery Agent, run `VDAWorkstationSetup.exe`
    - For the single-session OS Core Services Virtual Delivery Agent, run `VDAWorkstationCoreSetup.exe`

To extract the files before installing them, use `/extract` with the absolute path, for example `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. (The directory must exist. Otherwise, the extract fails.) Then in a separate command, run the appropriate command, using the valid options listed in this article.

- For `VDAServerSetup_XXXX.exe`, run `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- For `VDAWorkstationCoreSetup_XXXX.exe`, run `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- For `VDAWorkstationSetup_XXXX.exe`, run `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

Command-line options to install a VDA

The following options are valid with one or more of the commands: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, and `VDAWorkstationCoreSetup.exe`.

- **/components** *component*\[,*component*\]

  Comma-separated list of components to install or remove. Valid values are:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **VDA:** Virtual Delivery Agent
  - **PLUGINS:** Citrix Workspace™ app for Windows

  To install the VDA and Citrix Workspace app, specify `/components vda,plugins`.

  If the `plugins` option is left out, only the VDA is installed (not the Citrix Workspace app).

  This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer. That installer cannot install Citrix Workspace app.

- **/controllers** "*controller* ..."

  Space-separated FQDNs of Citrix Cloud Connectors with which the VDA can communicate, enclosed in straight quotation marks. Do not specify both the `/site_guid` and `/controllers` options.

- **/disableexperiencemetrics**

  Prevents the automatic upload of analytics collected during installation, upgrade, or removal to Citrix.

- **/enable_hdx_ports**

  Opens ports in the Windows firewall required by the VDA and enabled features (except Windows Remote Assistance), if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually. For port information, see Network ports.

  To open the UDP ports that HDX adaptive transport, specify the `/enable_hdx_udp_ports` option, in addition to the `/enable_hdx_ports` option.

- **/enable_hdx_udp_ports**

  Opens UDP ports in the Windows firewall that HDX adaptive transport requires, if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually. For port information, see Network ports.

  To open the ports that the VDA uses, specify the `/enable_hdx_ports` option, in addition to the `/enable_hdx_udp_ports` option.

- **/enable_real_time_transport**

  Enables or disables use of UDP for audio packets (RealTime Audio Transport for audio). Enabling this feature can improve audio performance. Include the `/enable_hdx_ports`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

option if you want the UDP ports opened automatically when the Windows Firewall Service is detected.

- **/enable_remote_assistance**

  Enables the shadowing feature in Windows Remote Assistance for use with the **Monitor** functions. If you specify this option, Windows Remote Assistance opens the dynamic ports in the firewall.

- **/enablerestore** or **/enablerestorecleanup**

  (Valid only for single-session VDAs) Enables automatic return to the restore point, if the VDA install or upgrade fails.

  If the install/upgrade completes successfully:

  - `/enablerestorecleanup` instructs the installer to remove the restore point.
  - `/enablerestore` instructs the installer to keep the restore point, even though it was not used.

  For details, see Restore on install or upgrade failure.

- **/enable_ss_ports**

  Opens ports in the Windows Firewall that are required for screen sharing, if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually.

- **/exclude** "*component*"\[,"*component*"\]

  Prevents installation of one or more comma-separated optional components, each enclosed in straight quotation marks. For example, installing or upgrading a VDA on an MCS-managed image needs the Machine Identity Service component. Valid values are:

  - Machine Identity Service
  - Citrix Profile Management
  - Citrix Profile Management WMI Plug-in
  - Citrix Personalization for App-V - VDA
  - Citrix MCS IODriver
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Excluding Citrix Profile Management from the installation (`/exclude "Citrix Profile Management"`) affects monitoring and troubleshooting of VDAs from the **Monitor** console. On the **User details** and **EndPoint** pages, the Personalization panel and the Logon Duration panel fail. On the **Dashboard** and **Trends** pages, the Average Logon Duration panel display data only for machines that have Profile Management installed.

Even if you are using a third-party Profile Management solution, Citrix recommends that you install and run the Citrix Profile Management Service. Enabling the Citrix Profile Management Service is not required.

If you plan to use MCS to provision VMs, do not exclude the Machine Identity Service.

If you specify both `/exclude` and `/includeadditional` with the same component name, the component isn't installed.

This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer. That installer automatically excludes many of these items.

- **/h** or **/help**

  Displays command help.

- **/includeadditional** "*component*"\[,"*component*"\] ...

  Includes installation of one or more comma-separated optional components, each enclosed in straight quotation marks. The component names are case-sensitive.

  This option can be helpful when you are creating a Remote PC Access deployment, and want to install components that are not included by default. Valid values are:

  - Citrix Profile Management
  - Citrix Profile Management WMI Plug-in
  - Citrix Personalization for App-V - VDA
  - Citrix MCS IODriver
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2
  - User personalization layer
  - Citrix Web Socket VDA Registration Tool

  If you specify both `/exclude` and `/includeadditional` with the same component name, that component isn't installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **/installdir** *directory*

  Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.

- **/install_mcsio_driver**

  Do not use. Instead, use `/includeadditional "Citrix MCS IODriver"` or `/exclude "Citrix MCS IODriver"`

- **/logpath** *path*

  Log file location. The specified folder must exist. The installer does not create it. Default = "%TEMP%\Citrix\XenDesktop Installer"

  This option isn't available in the graphical interface.

- **/masterimage**

  Valid only when installing a VDA on a VM. Sets up the VDA as an image. This option is equivalent to `/mastermcsimage`.

  This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer.

- **/mastermcsimage**

  Specifies that this machine will be used as an image with Machine Creation Services. This option is equivalent to `/masterimage`.

- **/masterpvsimage**

  Specifies that this machine will be used as an image with either Citrix Provisioning™ or a third-party provisioning tool (such as Microsoft System Center Configuration Manager).

- **/no_mediafoundation_ack**

  Acknowledges that Microsoft Media Foundation is not installed, and several HDX™ multimedia features are not installed and do not work. If this option is omitted and Media Foundation is not installed, the VDA installation fails. Most supported Windows editions come with Media Foundation already installed, except N editions.

- **/nodesktopexperience**

  Valid only when installing a multi-session OS VDA. Prevents enabling of the Enhanced Desktop Experience feature. This feature is also controlled with the Enhanced Desktop Experience Citrix policy setting.

- **/noreboot**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prevents a restart after installation. The VDA cannot be used until after a restart.

- **/noresume**

  By default, when a machine restart is needed during an installation, the installer resumes automatically after the restart completes. To override the default, specify `/noresume`. This can be helpful if you must remount the media or want to capture information during an automated installation.

- **/portnumber** *port*

  Valid only when the `/reconfig` option is specified. Port number to enable for communications between the VDA and the Controller. The previously configured port is disabled, unless it is port 80.

- **/proxyconfig** "*address or PAC file path*"

  Valid only if command contains `/includeadditional "Citrix Rendezvous V2"`. The address or PAC file path of the proxy for use with the Rendezvous protocol. For feature details, see Rendezvous protocol.

  - Proxy address format: `http://<url-or-ip>:<port>`
  - PAC file format: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** or **/passive**

  No user interface appears during the installation. The only evidence of the installation and configuration process is in Windows Task Manager. If this option is omitted, the graphical interface launches.

- **/reconfigure**

  Customizes previously configured VDA settings when used with the `/portnumber`, `/controllers`, or `/enable_hdx_ports` options. If you specify this option without also specifying the `/quiet` option, the graphical interface for customizing the VDA launches.

- **/remotepc**

  Valid only for Remote PC Access deployments (single-session OS) or brokered connections (multi-session OS).

  This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer. That installer automatically excludes installation of these components.

- **/remove_appdisk_ack**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authorizes the VDA installer to uninstall the AppDisks™ VDA plug-in if it's installed.

- **/remove_pvd_ack**

  Authorizes the VDA installer to uninstall Personal vDisk if it's installed.

- **/remove**

  Removes the components specified with the `/components` option.

- **/removeall**

  Removes the VDA. It does not remove the Citrix Workspace app (if installed).

- **/sendexperiencemetrics**

  Automatically sends analytics collected during the installation, upgrade, or removal to Citrix. If this option is omitted (or the `/disableexperiencemetrics` option is specified), analytics are collected locally, but not sent automatically.

- **/servervdi**

  Installs a single-session OS VDA on a supported Windows server. Omit this option when installing a multi-session VDA on a Windows server. Before using this option, see Server VDI.

- **/site_guid** *guid*

  Globally Unique Identifier of the site Active Directory Organizational Unit (OU). This associates a virtual desktop with a site when you are using Active Directory for discovery (auto-update is the recommended and default discovery method). The site GUID is a site property displayed in Studio. Do not specify both the `/site_guid` and `/controllers` options.

- **/tempdir** *directory*

  Directory to hold temporary files during installation. Default = c:\Windows\Temp.

  This option is not available in the graphical interface.

- **/virtualmachine**

  Valid only when installing a VDA on a VM. Overrides detection by the installer of a physical machine, where BIOS information passed to VMs makes them appear as physical machines.

  This option is not available in the graphical interface.

- **/xendesktopcloud**

  Indicates that the VDA is installed in a Citrix DaaS (Citrix Cloud™) deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Examples: Install a VDA

- **Install a VDA on a multi-session OS.** The following command installs a VDA on a multi-session OS.

  ```
  VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com" /
  enable_hdx_ports /masterimage
  ```

  The VDA will be used as an image.

- **Install a multi-session OS VDA or single-session OS VDA.** The following command installs a multi-session OS VDA or a single-session OS VDA.

  ```
  VDAServerSetup_XXXX.exe /quiet /controllers "ddc1.abc.com","ddc2.abc.com" /
  enable_hdx_ports /enable_Remote_Assistance /enable_real_time_transport /
  enable_ss_ports /noreboot
  ```

  Separate each delivery controller™ FQDN by a comma. Note that `XXXX` represents the VDA version.

- **Install a Core Services VDA on a single-session OS.** The following command installs a Core Services VDA on a single session OS for use in a Remote PC Access or VDA deployment.

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.domain.com" /
  enable_hdx_ports /noreboot
  ```

  Citrix Workspace app and other non-core services are not installed. The address of a Cloud Connector is specified, and ports in the Windows Firewall Service are automatically opened. The administrator handles restarts.

Customize a VDA using the command line

After you install a VDA, you can customize several settings. Run `XenDesktopVDASetup.exe`, using one or more of the following options.

- `/reconfigure` (required when customizing a VDA)
- `/h` or `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `/enable_hdx_ports`

Where to go next

- Create machine catalogs
- To review the entire configuration process, see Plan and build a deployment.

WebSocket communication between VDA and Delivery Controller™

This article describes how to set up a WebSocket connection for communication between VDAs and Delivery controllers as an alternative to using WCF communication. It provides the benefit that only the TLS port 443 for communication from the VDA to the Delivery Controller.

Currently this is only available for MCS provisioned machines.

How it works

The following section describes the workflow for the WebSocket connection between a Delivery Controller and a VDA:

1. The admins initiate the process by provisioning VDAs using the Machine Creation Service (MCS).
2. During the MCS provisioning process, MCS generates public-private key pairs for each VDA and registers the public keys with the FMA trust service on the Delivery Controller. MCS saves the public-private key pair as a file under the identity disk on the VDAs.
3. When the VDA machine boots up, the MCS agent installed on the VDA machine reads the key pair from the identity disk and writes this information to the VDA registry location.
4. The broker agent installed on the VDA reads the key pairs from the registry and generates an SSL-enabled WebSocket request to the Delivery Controller with a service key authentication header signed by the private key.
5. The delivery controller verifies the signed service key authentication header with the public key from the FMA trust service.
6. Once the verification is complete, the system establishes the WebSocket connection between the VDA and the Delivery Controller.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WebSocket support

Procedure

Follow the instructions to set up a WebSocket connection:

1. Create a machine catalog for AD-joined VDAs with MCS provisioning. For more information, see Create machine catalog.
2. Create a delivery group and add your VDA to it. For more information, see Create delivery groups.
3. Enable a WebSocket connection on the VDA. Run the following PowerShell command on the VDA:

   ```
   New-ItemProperty
   "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
   \WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

   - To check if WebSocket is enabled, check the following registry key value. The value of `Enabled` must be 1.

     Key:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
     nt\WebSocket
     ```

     Name: Enabled

     Type: REG_DWORD

     Value: 1

Create and manage connections

Introduction

Configuring a connection involves selecting the connection type from the list of supported hypervisors and cloud services, and choosing the appropriate storage and network resources for that connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You must have Full Administrator privileges to perform tasks related to connection and resource management.

Where to find information about connection types

System requirements provide a list of supported hypervisors and cloud service versions, along with links to articles for each specific host.

Host storage

A storage product is supported if it is manageable through a supported hypervisor. Citrix Support assists only those storage product vendors in troubleshooting and resolving issues, and documenting these issues and solutions in the Knowledge Center as necessary.

When provisioning machines, data is classified by type:

- Operating system (OS): includes images
- Temporary data: include all non-persistent data written to MCS-provisioned machines, Windows page files, and any data that is synchronized with ShareFile. This data is discarded each time a machine restarts. If the base image includes user profile data, this data remain persistent. If a centralized user profile solution is in use, the user profile data is synchronized with the external profile store. The locally cached user profile data is discarded upon each machine restart.

Allocating distinct storage resources for different types of data can minimize system load and enhance IOPS (Input/Output Operations Per Second) performance on each storage device. This strategic allocation makes optimal use of the host's available resources. Also, it allows for the selection of the most suitable storage medium based on the specific needs of each data type, such as greater persistence or resilience for certain kinds of data.

- Shared and local storage options: Storage resources can either be centralized that is, separate from any host and used by all hosts, or localized to a specific hypervisor. Centralized options include Windows cluster shared volumes, which might or might not have additional attached storage, or appliances from storage vendors. Centralized storage solutions might offer advanced features for optimizations, for example, hypervisor-specific storage control paths, and direct plug-in access.
- Local storage benefits and trade-offs: Storing temporary data locally avoids going to the network to access shared storage, thereby reduces IOPS load on the shared resources. While

© 1997–2026 Citrix Systems, Inc. All rights reserved.

centralized storage can be more expensive, using local storage can be a cost-effective alternative. However, these benefits can be weighed against the availability of sufficient storage on the hypervisor servers.

Storage shared by hypervisors

The storage shared by hypervisors method stores data that needs longer-term persistence centrally, providing centralized backup, and management. That storage holds the OS disks.

When you select this method, you can choose whether to use local storage (on servers in the same hypervisor pool) for temporary machine data. This data does not require persistence or as much resilience as the data in the shared storage. This is called the *temporary data cache*. The local disk helps reduce traffic to the main OS storage. This disk is cleared after every machine restart. The disk is accessed through a write-through memory cache. Keep in mind that if you use local storage for temporary data, the provisioned VDA is tied to a specific hypervisor host. If that host fails, the VM cannot start.

Exception: If you use Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager does not allow temporary data cache disks to be created on local storage.

If you store temporary data locally, you can then enable and configure non-default values for each VM's cache disk and memory size when you create a machine catalog that uses that connection. However, the default values are as per the connection type, and are sufficient for most cases.

The hypervisor can also provide optimization technologies through in-memory read-caching of the disk images locally. For example, XenServer offers IntelliCache. This can also reduce network traffic to the central storage.

Storage local to the hypervisor

The storage local to the hypervisor method stores data locally on the hypervisor. With this method, images and other OS data are transferred to all the hypervisors used in the site, both for initial machine creation and future image updates. This results in significant traffic on the management network. Image transfers are also time-consuming, and the images become available to each host at a different time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a connection and resources

IMPORTANT:

The host resources (storage and network) in your resource location must be available before you create a connection.

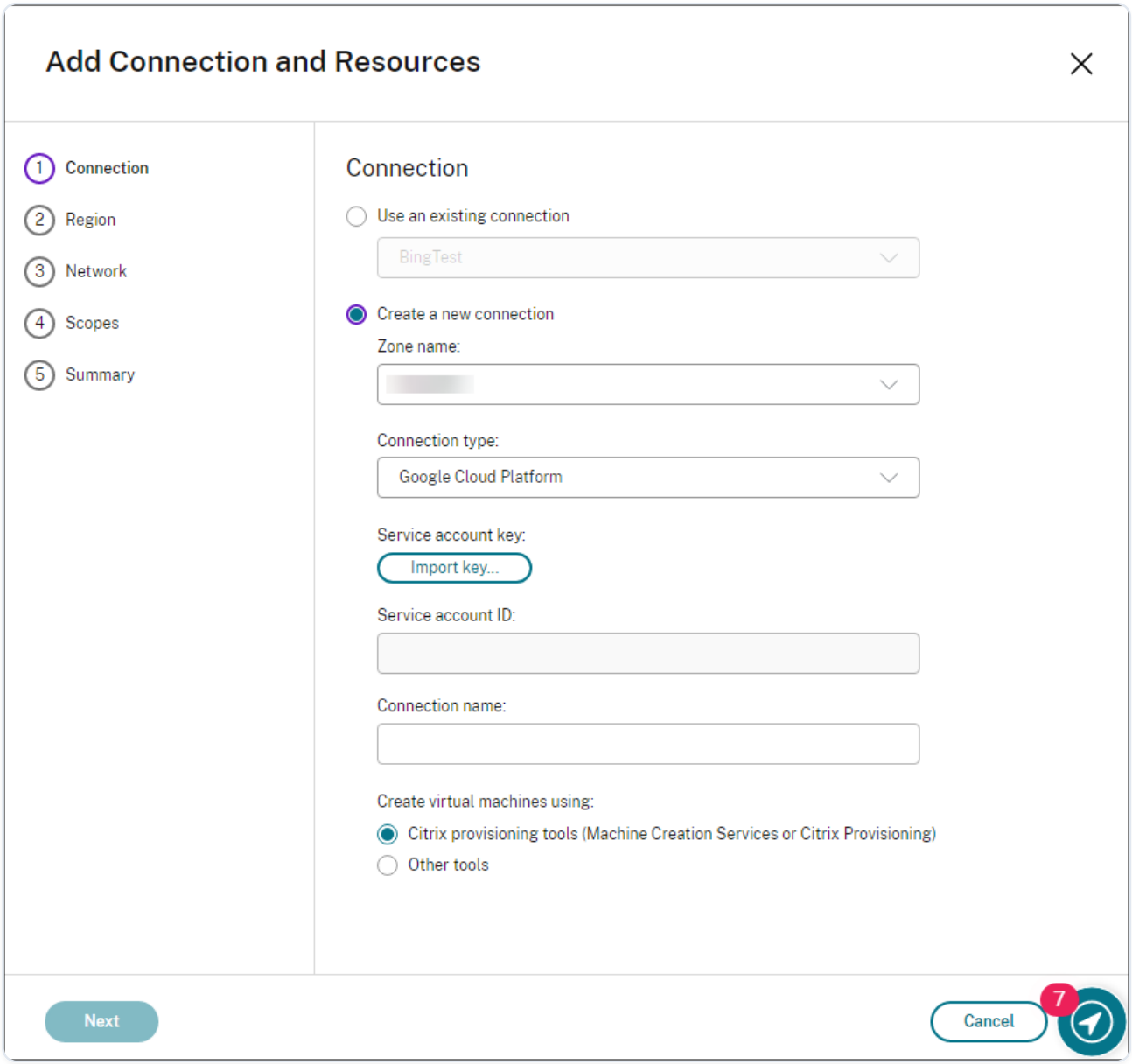
1. Sign in to Citrix Cloud.
2. In the **DaaS** tile, click **Manage** to open Studio.
3. Select **Hosting** in the left pane.
4. Click **Add Connections and Resources** in the action bar.
5. The wizard guides you through the configuration process described in the following steps. Specific page content depends on the selected connection type. After completing the steps on each page, select **Next** until you reach the **Summary** page.

NOTE:

The content of each page within the wizard varies based on the type of connection that you've selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1. Connection



On the **Connection** page:

- To create a new connection, select **Create a new Connection**. To create a resource for an existing connection, select **Use an existing Connection**, and then choose the relevant connection.
- Select a zone in the **Zone name** field. The options are all resource locations you configured.
- Select a hypervisor or cloud service in the **Connection type** field. The options include all Citrix-supported hypervisors and cloud services:
  - For a resource location without accessible Cloud Connectors, only hypervisors and cloud services that support connectorless deployments are available.
  - For a resource location with accessible Cloud Connectors, only hypervisors and cloud services that have their plug-ins properly installed on those connectors are available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

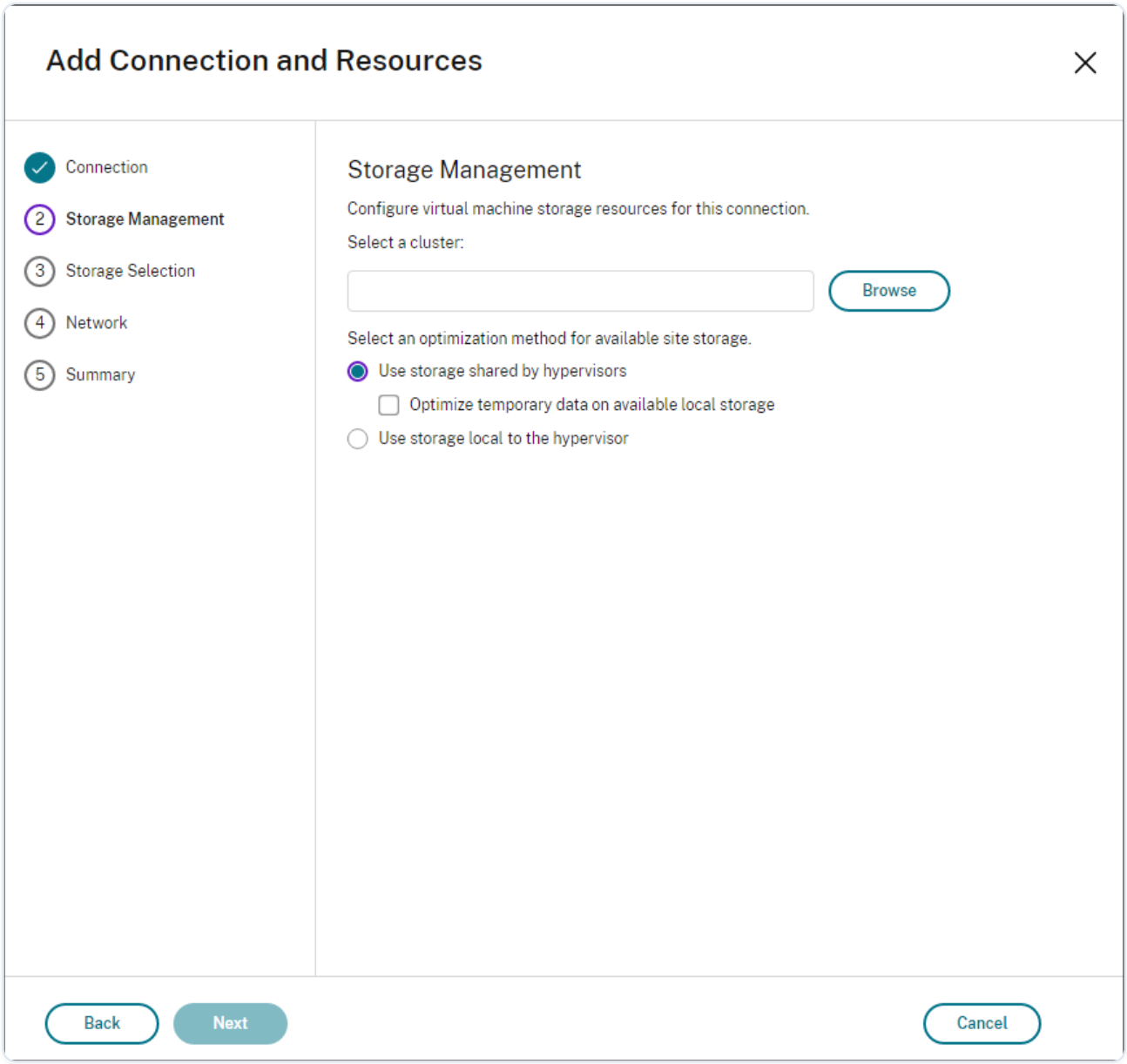
Alternatively, you can use the PowerShell command `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false or true to get the list of available hypervisors and Cloud services.

- Enter a connection name. This name appears in the **Hosting** display.
- Choose a tool to create virtual machines.

NOTE:

Information on the **Connection** page differs depending on the host or connection type that you're using. For example, when using Azure Resource Manager, you can use choose either a service principal or managed identity. For details, see Connection to Microsoft Azure.

Step 2. Storage management



© 1997–2026 Citrix Systems, Inc. All rights reserved.

For information about storage management types and methods, see Host storage.

If you are configuring a connection to a Hyper-V or VMware host, browse to and then select a cluster name. Other connection types do not request a cluster name.

Select a storage management method: storage shared by hypervisors or storage local to the hypervisor.

For more information, see Storage shared by hypervisors and Storage local to the hypervisor.

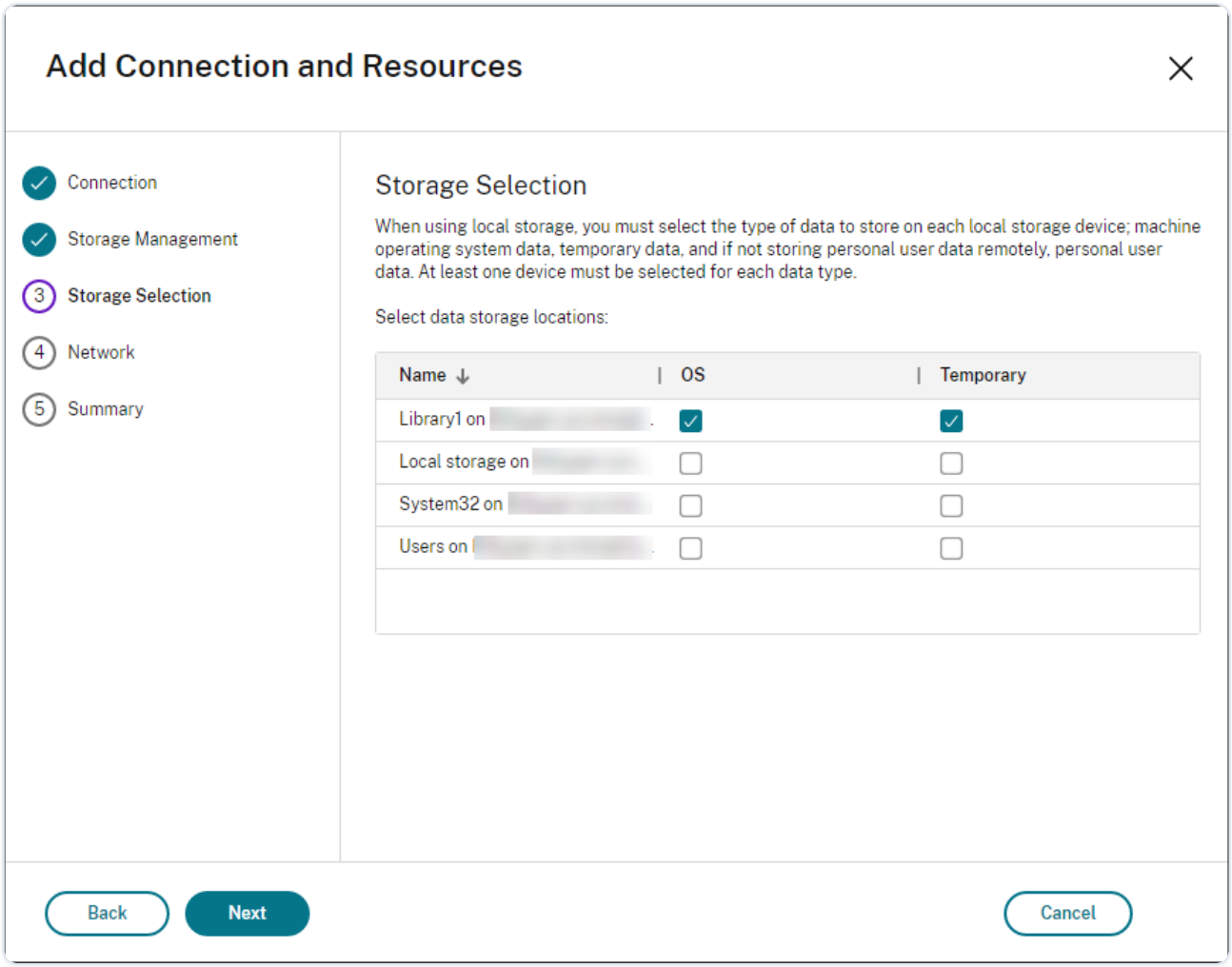
If you use shared storage on a XenServer pool, indicate if you want to use IntelliCache to reduce the load on the shared storage device. See Use IntelliCache for XenServer connections.

NOTE:

In XenServer®, VMware, and SCVMM virtualization environments, you can have Write-back cache (WBC) disk on the same storage location as OS disk. For this, do not select **Optimize temporary data on available local storage**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3. Storage selection



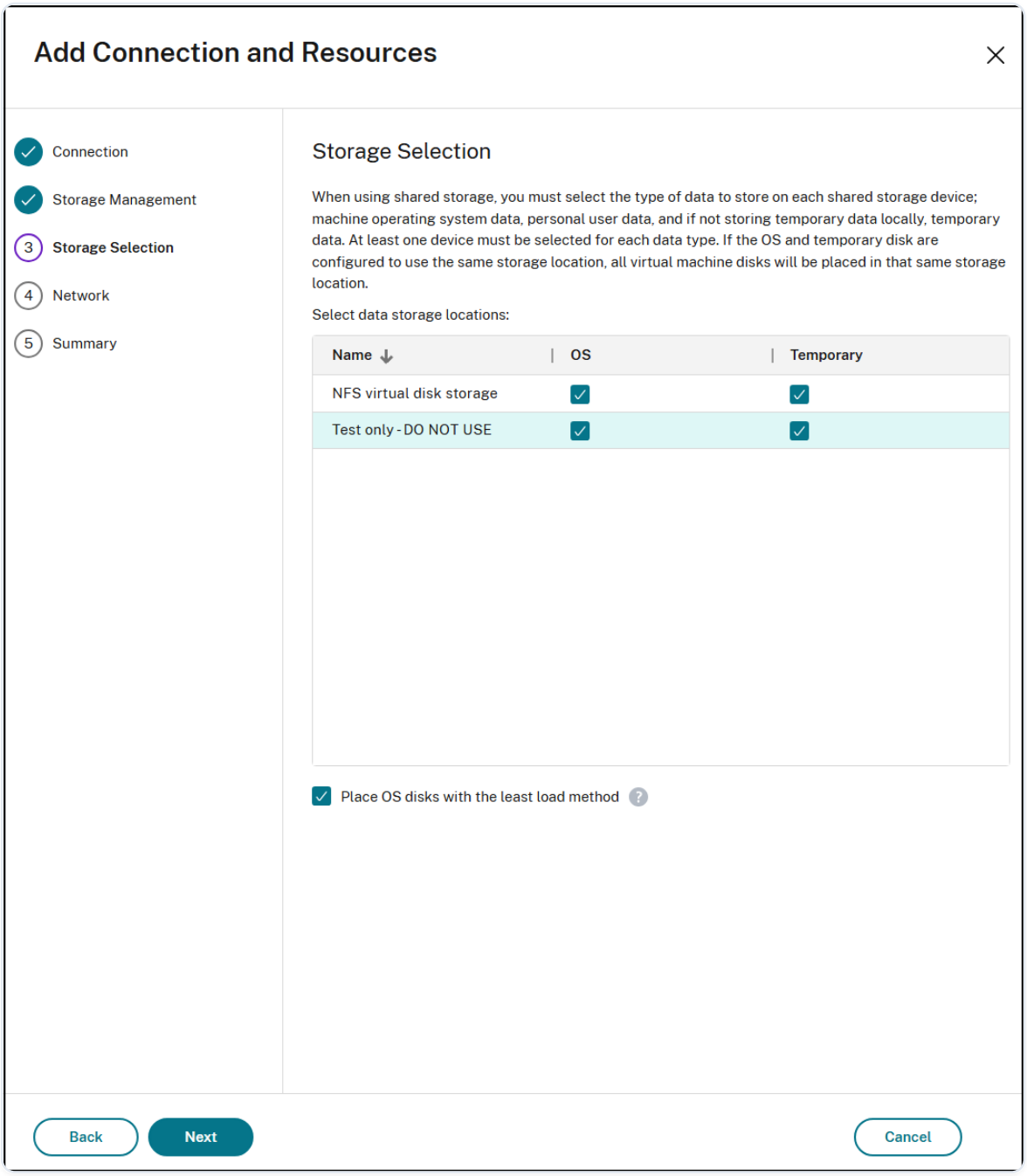
For more information about storage selection, see Host storage.

Select at least one host storage device for each available data type. The storage management method that you selected on the previous page affects which data types are available for selection on this page. You must select at least one storage device for each supported data type before you can proceed to the next page in the wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- In XenServer, VMware, and SCVMM virtualization environments, MCS places Write-back cache (WBC) disk on the same storage location as OS disk if you configure the available OS storage list the same as the available temporary storage list.
- If you select at least two or more OS data storage locations, the **Optimize storage load balancing with least load method option** appears. This option allows you to choose the least loaded storage repository for disk allocation.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **Summary** page indicates whether the option is **Enabled** or **Disabled**, depending on your selection. The **Details** panel displays changes to the storage allocation method. You can adjust it using the **Edit storage** option on the **OS Storage** page.

You can get more configuration options on **Storage Selection** page if you choose **Use storage shared by hypervisors** and select **Optimize temporary data on available local storage** on **Storage Management** page. For example, you can select which local storage devices (in the same hypervisor pool) to use for temporary data.

The number of currently selected storage devices is shown (in the graphic, "1 storage device selected"). When you hover over that entry, the selected device names appear (unless no devices are configured).

1. Select **Select** to change the storage devices to use.
2. In the **Select Storage** dialog box, select or clear the storage device checkboxes, and then select **OK**.

Step 4. Region

NOTE:

The **Region** page appears only for some host types.

The region selection indicates where VMs will be deployed. Ideally, choose a region close to where users will access their applications.

Step 5. Network

Enter a name for the resources. This name identifies the storage and network combination associated with the connection.

Select one or more networks that the VMs will use.

Some connection types (such as Azure Resource Manager) also list subnets that VMs will use. Select one or more subnets.

Step 6. Summary

Review your selections. If you want to make changes, return to the previous wizard pages. When you complete your review, select **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- If you store temporary data locally, you can configure non-default values for temporary data storage when you create the catalog containing machines that use this connection.
- A scope is not shown for Full access administrators. For more information, see Administrators, roles, and scopes.

Edit connection settings

You cannot use this procedure to:

- Rename a connection or create a new connection.
- Change the GPU settings for a connection. Catalogs accessing this resource must use an appropriate GPU-specific image. Therefore, if you want to change the GCP settings, create a new connection instead of editing an existing connection.

Edit a connection

1. From Studio, select **Hosting** in the left pane.
2. Select the connection and then select **Edit Connection** in the action bar.
3. Use the **Connection Properties** page to change the connection address and credentials. Change the address only if the current host machine has a new address. Entering an address to a different machine breaks the connection's machine catalogs.
    - Select **Edit settings…**, and then enter the new information.
    - To specify the high-availability servers for a XenServer connection, select **Edit servers...** and select the servers. Citrix recommends that you select all servers in the pool to allow communication with XenServer if the pool master fails.

    NOTE:

    If you are using HTTPS and want to configure high-availability servers, do not install a wildcard certificate for all servers in a pool. An individual certificate for each server is required. For more information, see Create a connection to XenServer.
4. Use the **Advanced** page to edit the settings to specify a maximum number of simultaneous actions (or concurrent machines) per hosting connection. These settings can help when power

© 1997–2026 Citrix Systems, Inc. All rights reserved.

management settings allow too many or too few machines to start at the same time. Each connection type has specific default values that are appropriate for most cases. Usually, they do not need to be changed.

- The **Simultaneous actions (all types)** and **Simultaneous Personal vDisk inventory updates** settings specify two values: a maximum absolute number that can occur simultaneously on this connection, and a maximum percentage of all machines that use this connection. You must specify both absolute and percentage values. The actual limit applied is the lower of the values.

  For example, in a deployment with 34 machines, if **Simultaneous actions (all types)** is set to an absolute value of 10 and a percentage value of 10, the actual limit applied is 3 (that is, 10 percent of 34 rounded to the nearest whole number, which is less than the absolute value of 10 machines).
- The **Maximum new actions per minute** is an absolute number. There is no percentage value.
- Enter information in **Connection options** only under the guidance of a Citrix Support representative.

5. Use the **Scopes** page to select one or more scopes for this host.

   NOTE:

   A scope is not shown for Full access administrators. By definition, those administrators can access all customer-managed Citrix Cloud and subscribed services objects.

   For more information, see Administrators, roles, and scopes.
6. Use the **Shared Tenants** page to add tenants and subscriptions that share the Azure Compute Gallery with the subscription of this connection.

   a. Enter the **Application secret** for the application associated with this connection. With this information, you can authenticate to Azure. We recommend that you change keys regularly to ensure security.

   b. Add shared tenants and subscriptions. You can add up to eight shared tenants. For each tenant, you can add up to eight subscriptions.
7. Click **Save** and **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Turn maintenance mode on or off for a connection

Turning on maintenance mode for a connection prevents any new power action from affecting any machine stored on the connection. Users cannot connect to a machine when it is in maintenance mode. If users are already connected, maintenance mode takes effect when they log off.

1. From Studio, select **Hosting** in the left pane.
2. Select the connection. To turn maintenance mode on, select **Turn On Maintenance Mode** in the action bar. To turn maintenance mode off, select **Turn Off Maintenance Mode**.

You can also turn the maintenance mode on or off for individual machines. You can turn maintenance mode on or off for machines in machine catalogs or delivery groups.

Delete a connection

CAUTION:

Deleting a connection can result in the deletion of large numbers of machines and loss of data. Ensure that user data on affected machines is backed up or no longer required.

Before deleting a connection, ensure that:

- All users are logged off from the machines stored on the connection.
- No disconnected user sessions are running.
- Maintenance mode is turned on for pooled and dedicated machines.
- All machines in machine catalogs used by the connection are powered off.

A machine catalog becomes unusable when you delete a connection that the catalog references. If this connection is referenced by a catalog, you can delete the catalog. Before you delete a catalog, make sure it is not used by other connections.

1. From Studio, select **Hosting** in the left pane.
2. Select the connection and then select **Delete Connection** in the action bar.
3. If this connection has machines stored on it, you are asked whether to delete the machines. If they are to be deleted, specify what to do with the associated Active Directory computer accounts.

Rename a connection

1. From Studio, select **Hosting** in the left pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the connection and then select **Rename Connection**.

Test a connection

1. From Studio, select **Hosting** in the left pane.
2. Select the connection and then select **Test Connection**.

Test TLS Certificate

1. From Studio, select **Hosting** in the left pane.
2. Right-click the connection for which you want to re-trust the certificate with a warning symbol and select **Test TLS Certificate Trust**.
3. Input the password in the subsequent window and click **Save**.
    a. If the certificate needs to be re-trusted, a warning dialog box pops up with an option to trust the certificate.
    b. If the certificate is already trusted, a successful dialog box pops up that says the certificate is trusted.

View machine details on a connection

1. From Studio, select **Hosting** in the left pane.
2. Select the connection and then select **View Machines** in the action bar.

The upper pane lists the machines accessed through the connection. Select a machine to view its details in the lower pane. Session details are also provided for open sessions.

Use the search feature to find machines quickly. Either select a saved search from the list at the top of the window, or create a new search. You can either search by typing all or part of the machine name, or you can build an expression to use for an advanced search. To build an expression, select **Unfold**, and then select from the lists of properties and operators.

Manage machines on a connection

1. From Studio, select **Hosting** in the left pane.
2. Select a connection and then select **View Machines** in the action bar.
3. Select one of the following in the action bar. Some actions might not be available, depending on the machine state and the host connection type.
    - **Start:** Starts the machine if it is powered off or suspended.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Suspend:** Pauses the machine without shutting it down, and refreshes the list of machines.
- **Shut down:** Requests the operating system to shut down.
- **Force shut down:** Forcibly powers off the machine, and refreshes the list of machines.
- **Restart:** Requests the operating system to shut down and then start the machine again. If the operating system cannot comply, the desktop remains in its current state.
- **Enable maintenance mode:** Temporarily stops connections to a machine. Users cannot connect to a machine in this state. If users are connected, maintenance mode takes effect when they log off. (You can also turn maintenance mode on or off for all machines accessed through a connection, as described earlier.)
- **Remove from Delivery Group:** Removing a machine from a Delivery Group does not delete it from the machine catalog that the Delivery Group uses. You can remove a machine only when no user is connected to it. Turn on maintenance mode to temporarily prevent users from connecting while you are removing the machine.
- **Delete:** When you delete a machine, users no longer have access to it, and the machine is deleted from the machine catalog. Before deleting a machine, ensure that all user data is backed up or no longer required. You can delete a machine only when no user is connected to it. Turn on maintenance mode to temporarily stop users from connecting while you are deleting the machine.

For actions that involve machine shutdown, if the machine does not shut down within 10 minutes, it is powered off. If Windows attempts to install updates during shutdown, there is a risk that the machine will be powered off before the updates are completed.

Edit storage

You can display the status of servers that are used to store the operating system, temporary, and personal (PvD) data for VMs that use a connection. You can also specify which servers to use for storage of each data type.

1. From Studio, select **Hosting** in the left pane.
2. Select the connection and then select **Edit Storage** in the action bar.
3. In the left pane, select the data type: operating system or temporary.
4. Select or clear the checkboxes for one or more storage devices for the selected data type.
5. Select **OK**.

Each storage device in the list includes its name and storage status. Valid storage status values are:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **In use**: The storage is being used for creating machines.
- **Superseded**: The storage is being used only for existing machines. No new machines are added to this storage.
- **Not in use**: The storage is not being used for creating machines.

If you clear the checkbox for a device that is currently **In use**, its status changes to **Superseded**. Existing machines will continue to use that storage device (and can write data to it). So, that location can become full even after it stops being used for creating machines.

Detect Orphaned Azure resources

Orphaned resources are unused resources present in the system and they can lead to unnecessary expenses.

Apart from Cloud administrators, any newly created roles with **Use Host Connection to Detect Orphaned Resources in Hypervisor** permission under **Hosts** will be able to detect orphaned resources.

This feature allows you to detect the orphaned Azure resources in the hosts on your cloud site.

Follow the steps on Citrix DaaS™:

1. From Studio, select **Hosting** in the left pane.
2. Select a connection, and then select **Detect Orphaned Resources** in the action bar. The **Detect Orphaned Resources** dialog box displays the orphaned resource report.
3. To view the orphaned resource report, select **View Report**.

Alternatively, you can detect orphaned Azure resources using PowerShell. For more information, see Retrieve a list of orphaned resources.

To understand the reasons behind the orphaned resources, and to learn how to proceed further, see Efficiently manage Orphaned Azure resources with Citrix.

Connection timers

You can use Citrix policy settings to configure three connection timers:

- **Maximum connection timer:** Determines the maximum duration of an uninterrupted connection between a user device and a virtual desktop. Use the **Session connection timer** and **Session connection timer interval** policy settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Connection idle timer:** Determines how long an uninterrupted user device connection to a virtual desktop is maintained if there is no input from the user. Use the **Session idle timer** and **Session idle timer interval** policy settings.
- **Disconnect timer**: Determines how long a disconnected, locked virtual desktop can remain locked before the session is logged off. Use the **Disconnected session timer** and **Disconnected session timer interval** policy settings.

When you update any of these settings, ensure they are consistent across your deployment.

See the policy settings documentation for more information.

Edit networks of resources

You can change networks for a connection. Do the following:

1. Go to **Hosting**.
2. Select the target resources under the connection and then select **Edit Network** in the action bar.
3. Select one or more networks for the virtual machines to use.
4. Click **Save** to save your changes and exit.

Delete, rename, or test resources

1. From Studio, select **Hosting** in the left pane.
2. Select the target resources under the connection, and then select the appropriate entry in the action bar:
    - **Delete Resources**
    - **Rename Resources**
    - **Test Resources**

Flexible storage location option for VMs

The VMs in a machine catalog are allocated various storage services (SR). To balance the VM allocation in different storage, you have two options:

- **Enhanced current round robin allocation method**: Instead of always starting from the same fixed SR, MCS begins the allocation from the SR right after the last used SR.
- **Least load-based allocation method**: Places the VMs on the least current load, determined by comparing the total number of VMs on each SR within the same machine catalog. For

© 1997–2026 Citrix Systems, Inc. All rights reserved.

example, if a machine catalog contains 100 VMs distributed as follows: 20 VMs on SR1, 30 VMs on SR2, and 50 VMs on SR3, the new VMs are allocated to SR1 first. This method ensures that the load across SR1, SR2, and SR3 is balanced.

This feature is:

- Applicable to all on-premises hypervisors (VMware, XenServer, and Hyper-V)
- Applicable to only OS disk storage.
- Not applicable to the existing VMs

To implement the load-based allocation option, add the custom property `Name="StorageBalanceType"` `Value="VMCountBasedLeastLoad` while creating or updating a host connection. If you don't use this custom property and value, then by default the enhanced round robin method is applied.

For example:

- While creating a host connection:

```
New-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>"
-HypervisorConnectionName "Xen-Connection" -NetworkPath @("XDHyp:
\Connections\Xen-Connection\Network 0.network") -Path @("XDHyp:
\HostingUnits\XS-Network") -PersonalvDiskStoragePath @() -RootPath
"XDHyp:\Connections\Xen-Connection\" -StoragePath @("XDHyp:
\Connections\Xen-Connection\NFS virtual disk storage.storage")
```

- While updating a host connection:

```
Set-Item  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>" -Path @("XDHyp:
\HostingUnits\XS-Network")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Retrieve a list of orphaned resources

You can get a list of orphaned resources that are created by MCS but are no longer tracked by MCS. This is currently applicable to Azure environments. To get the list, you can use PowerShell commands. You can filter using connections.

By default, the **Full Administrator** and **Cloud Administrator** roles have this permission assigned. To allow other roles to perform this action, assign them the **Use Host Connection to Detect Orphaned Resources in Hypervisor** permission under **Hosts**. For more information, seeCreate and manage roles.

NOTE:

The PowerShell command is rejected if any provisioning or image update is in progress.

Limitations

- To avoid incorrect recognition of orphaned resources, do not power on VMs while you are filtering orphaned resources.
- Around 2,000 records are displayed as orphaned if there is possible heavy workload.

Display the list of orphaned resources

To display the list of orphaned resources

1. Open a **PowerShell** window.
2. Run `asnp citrix*`.
3. Run the following commands:

    a. Get the connection uid. The connection uid is the value of the HypervisorConnectionUid attribute.

    ```
    Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
    'Azure*' }"
    ```

    b. Get the list of orphaned resources.

    ```
    get-provorphanedresource

    -HypervisorConnectionUid <connection uid>
    ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Display the list of orphaned resources from a subscription id

To display the list of orphaned resources from a subscription id:

1. Open a **PowerShell** window.
2. Run `asnp citrix*`.
3. Run the following commands:

    a. Find the connection uid using the subscription ID. The connection uid is the value of the HypervisorConnectionUid attribute.

    ```
    Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
    -match '<subscriptionId>' }
    ```

    b. Get the list of orphaned resources.

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

NOTE:

Check the resources carefully before deleting.

Use WinHttp (netsh) proxy server settings for hosting connection

This feature enhancement allows hosting connections to use the WinHttp (netsh) proxy server settings to be used with the hosting connection. This allows simpler proxy setup and also ensures consistent proxy usage between the Cloud Connector and host connections.

This feature is applicable to the following virtualization environments:

- Nutanix
- HPE Moonshot
- Red Hat OpenShift

Use cases

- Example 1: No custom property is set on the hosting connection

  The hosting connection will not read any proxy configuration settings on the machine and will attempt to connect to the hypervisor without a proxy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Example 2: Custom property is set on the hosting connection with value = True

  The hosting connection will only read the WinHttp proxy settings and use the proxy settings if present. If not present, no proxy settings will be used for the hosting connection.

- Example 3: Custom property is set on the hosting connection with value = False

  The hosting connection will not read any proxy configuration settings on the machine and will attempt to connect to the hypervisor without a proxy.

Changes to the existing workflow or process

- To use the WinHttp (netsh) proxy server configured on the Cloud Connectors for the hosting connection, you can now include this custom property with the hosting connection.

  ```
  <Property xsi:type="StringProperty"
  Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />
  ```

- When this custom property is set to `True`, the API calls to the hypervisor are routed through the WinHttp proxy server set on the machine through netsh winhttp set proxy command.
- When this custom property is set to `False`, or this custom property is not set, the API calls will ignore all the proxy servers (including the WinINet proxy and .net proxy) configured on the Cloud Connectors.

Prerequisite

Before setting the custom property while creating the host connection using PowerShell, make sure that you configure the WinHTTP proxy on all the Citrix Cloud Connectors in the Resource Location.

Configuration steps

To create a new hosting connection to use the WinHttp proxy settings through CLI:

```
$CustomProperties = "<CustomProperties  xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<!-- Include any other hypervisor specific custom properties here -->

<Property xsi:type=`"StringProperty`"
Name=`"UseSystemProxyForHypervisorTrafficOnConnectors`" Value=`"True`" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</CustomProperties>"



New-Item -ConnectionType $ConnectionType -HypervisorAddress @('https://
hypervisorhost1.example.com') -Path @('XDHyp:\Connections\
$ConnectionName') -Password $Password -UserName $User -CustomProperties
$CustomProperties
```

To set the custom property on an existing hosting connection:

1. Copy the existing custom properties from the host connection if any present.

   ```
   dir XDHyp:\Connections
   ```

2. Copy the custom properties for your host connection and add the following, and save it to a variable.

   ```
   $CustomProperties

   <Property xsi:type=`"StringProperty`"
   Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />
   ```

   Example:

   ```
   $CustomProperties = "<CustomProperties xmlns=`"http://
   schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
   www.w3.org/2001/XMLSchema-instance`">

   <Property xsi:type=`"IntProperty`"
   Name=`"MaximumConcurrentProvisioningOperations`" Value=`"100`"/
   ><Property xsi:type=`"StringProperty`"
   Name=`"UseSystemProxyForHypervisorTrafficOnConnectors`"
   Value=`"True`" />

   </CustomProperties>"
   ```

   If existing custom property was empty, set the custom property:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$CustomProperties = "<CustomProperties  xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`"
Name=`"UseSystemProxyForHypervisorTrafficOnConnectors`"
Value=`"True`" />

</CustomProperties>"
```

3. Run `Set-Item` command to update the existing hosting connection.

```
Set-Item -CustomProperties $CustomProperties -LiteralPath @("XDHyp:
\Connections\$ConnectionName") -PassThru -UserName $User
-SecurePassword $Password
```

Where to go next

- For information on connection to specific host types, see:
  - Connection to AWS
  - Connection to Google cloud environments
  - Connection to Microsoft Azure
  - Connection to Microsoft System Center Virtual Machine Manager
  - Connection to Nutanix
  - Connection to Nutanix cloud and partner solutions
  - Connection to VMware
  - Connection to VMware cloud and partner solutions
  - Connection to XenServer

If you're in the initial deployment process, create a machine catalog.

Connection to Amulet Hotkey CoreStation

Create and manage connections and resources describes the general wizards for creating a connection. The following information covers details specific to Amulet Hotkey CoreStation. You can currently create a connection to the Amulet Hotkey CoreStation using PowerShell commands.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Before creating a connection to Amulet Hotkey CoreStation, you need to first finish setting up your Amulet Hotkey CoreStation account. See Amulet Hotkey CoreStation virtualization environments

Create a connection

You can create a connection to Amulet Hotkey CoreStation using:

- Studio
- PowerShell commands

Create a connection using Studio

1. In the **Add Connection and Resources** page, select **Amulet Hotkey CoreStation** as the connection type.
2. Enter the connection address of your Amulet Hotkey CoreStation enclosure Manager. You can use an IP address, host name, or FQDN for the address.
3. Enter your enclosure administrative credentials and a friendly connection name.

   Connection setup stops when either of the situations occurs:

   - DaaS receives a public CA-signed certificate with errors: An error message appears. Follow the on-screen instructions to fix the issue. Otherwise, you can't proceed with connection creation.
   - DaaS receives a private CA-signed certificate: A warning page appears. Compare the received thumbprint with the server's for the certificate validity. If it's valid, select Trust certificate and click OK to proceed with connection creation. DaaS will then trust the certificate and store the thumbprint for future validation.

Create a connection using PowerShell commands

When you create a connection using PowerShell command, provide the following information:

- IP: Amulet Hotkey CoreStation IP Address
- Username: Amulet Hotkey CoreStation username
- Password: Amulet Hotkey CoreStation password

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-ConfigZone

Get-HypHypervisorPlugin

New-Item `

    -ConnectionType "Custom" `

    -HypervisorAddress $IP `

    -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} `

    -Path @("XDHyp:\Connections\$connectionName") `

    -Persist `

    -PluginId "AmuletHotkeyCoreStationFactory" `

    -Scope @() `

    -SecurePassword $Password `

    -UserName $UserName `

    -ZoneUid $ZoneUid `

    -SslThumbprint $SslThumbprint

New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$HypervisorConnectionID
```

NOTE:

The `-SslThumbprint` parameter is required only for private CA-signed certificates.

Certificate and thumbprint validation

For creating a successful connection to Amulet Hotkey CoreStation, the certificate must not have errors and the thumbprint must have a correct value. Following are the use cases related to the certificate and thumbprint validation:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCENARIO	RESULT
Public CA-signed certificate has errors.	The connection is not created successfully. See the error details and resolve the issue.
Public CA-signed certificate without errors.	The connection is created successfully, and the `SslThumbprints` value is `Null`.
Private CA-signed certificate without errors and a `sslthumbprint` value.	The connection is created successfully with a correct `SslThumbprints` value.
Private CA-signed Certificate with an incorrect thumbprint value.	The connection is not created successfully.
Private CA-signed Certificate without errors. (no thumbprint provided)	The connection is created successfully. The `SSlThumbprints` is `Null` when creating the connection. The `SSlThumbprints` value is updated to a value by the site service.

Manage connections

Fix certificate issues

Citrix DaaS blocks an Amulet Hotkey CoreStation connection when certificate issues arise, preventing you from delivering and managing workloads on associated Amulet Hotkey CoreStation nodes. You'll see an error icon next to the connection in the **Host connections** list.

See the following table for specific issues and solutions.

ISSUE	SOLUTION
A certificate error occurs to the public CA-signed certificate.	Click the connection and select the **Troubleshoot** tab. View the error details and resolve the issue.
The received certificate is private CA-signed or expired.	Edit the host connection to update the certificate thumbprint. Details steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE	SOLUTION	
	1. Select the connection and click **Edit Connection**. 2. On the **Connection Properties** page, click **Edit settings**. 3. Enter the password to connect to the Amulet Hotkey CoreStation enclosure, and then click **Save**. 4. On the **Warning** page that appears, compare the received thumbprint with the server's for certificate validity. 5. If they are the same, select **Trust certificate** and then click **OK**.	

Update thumbprint value

After creating the connection, you can update the thumbprint value of a connection using the `Set-Item` PowerShell command. Follow the steps to update the thumbprint value.

1. Get the connection details of a connection. For example:

```
Get-Item -LiteralPath xdhyp:\connections\AmuletCon-101
```

2. Update the thumbprint value. For example:

```
Set-Item -LiteralPath xdhyp:\connections\AmuletCon-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. Check the updated thumbprint value. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-Item -LiteralPath xdhyp:\connections\AmuletCon-101
```

NOTE:

The update fails if you provide an incorrect thumbprint value in the `Set-Item` command.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For Amulet Hotkey CoreStation information, see Create an Amulet Hotkey CoreStation machine catalog

More information

- Create and manage connections and resources
- Amulet Hotkey CoreStation virtualization environments

Connection to AWS EC2

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to AWS cloud environments.

Prerequisites

Do the following before creating a connection to AWS EC2:

- Complete setting up your AWS as a resource location. See AWS virtualization environments.
- Define IAM permissions policy of IAM user or role for Citrix to manage AWS resources on your behalf.

Define IAM permissions

Before creating a host connection, an IAM permissions policy needs to be properly defined for an IAM user or role that gives Citrix proper permissions to provision and manage resources in your AWS account on your behalf. Use the information in this section to define IAM permissions for Citrix DaaS on AWS. Amazon's IAM service permits accounts having multiple users, which can be further organized into groups. These users can possess different permissions to control their ability to perform operations associated with the account. For more information about IAM permissions, see the IAM JSON policy reference.

To apply IAM permissions policy to a new group of users:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Log in to the AWS management console and select the **IAM service** from the drop-down list.
2. Select **Create a New Group of Users**.
3. Type a name for the new user group and select **Continue**.
4. On the **Permissions** page, choose **Custom Policy** then **Select**.
5. Type a name for the **Permissions policy**.
6. In the **Policy Document** section, enter the relevant permissions.

After entering the policy information, select **Continue** to complete the application of the IAM permissions policy to the group of users. Users in the group are granted permissions to do only those actions that are required for Citrix DaaS.

IMPORTANT:

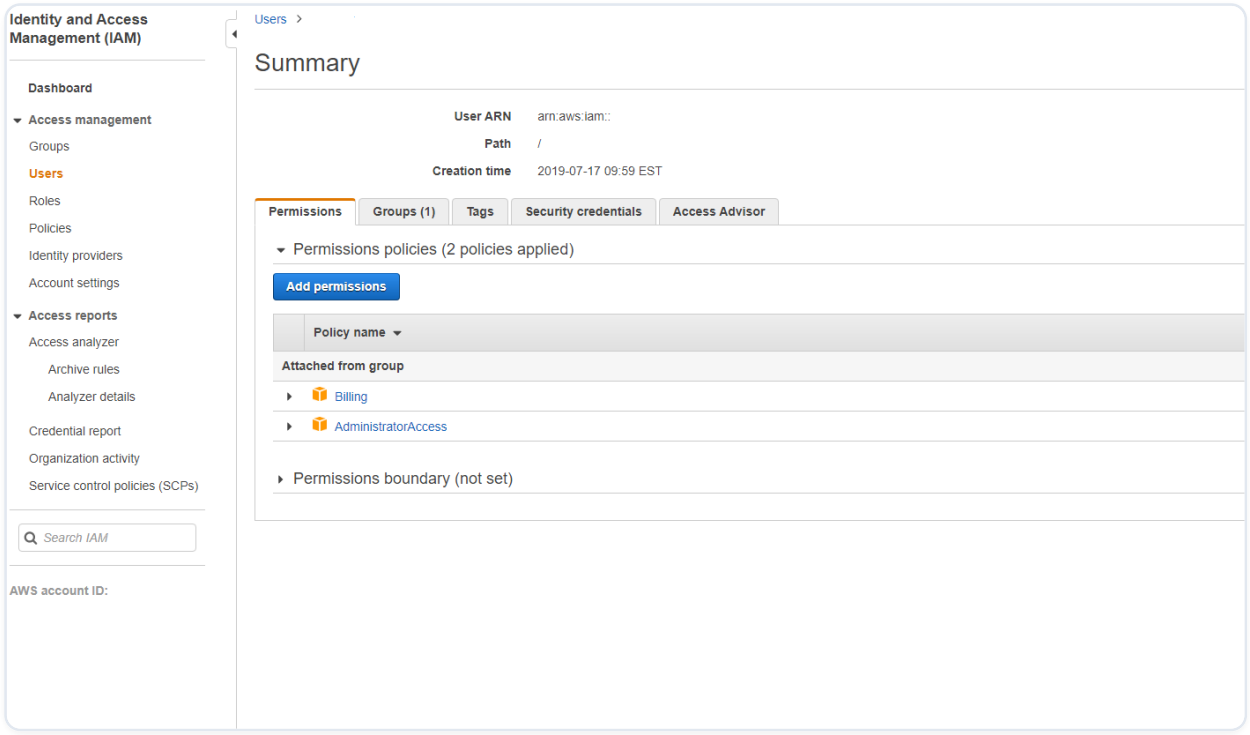
Use the policy text provided in the example provided in this article to list the actions that a Citrix DaaS uses to perform actions within an AWS account without restricting those actions to specific resources. Citrix recommends that you use the example for testing purposes. For production environments, you might choose to add further restrictions on resources.

Add IAM permissions

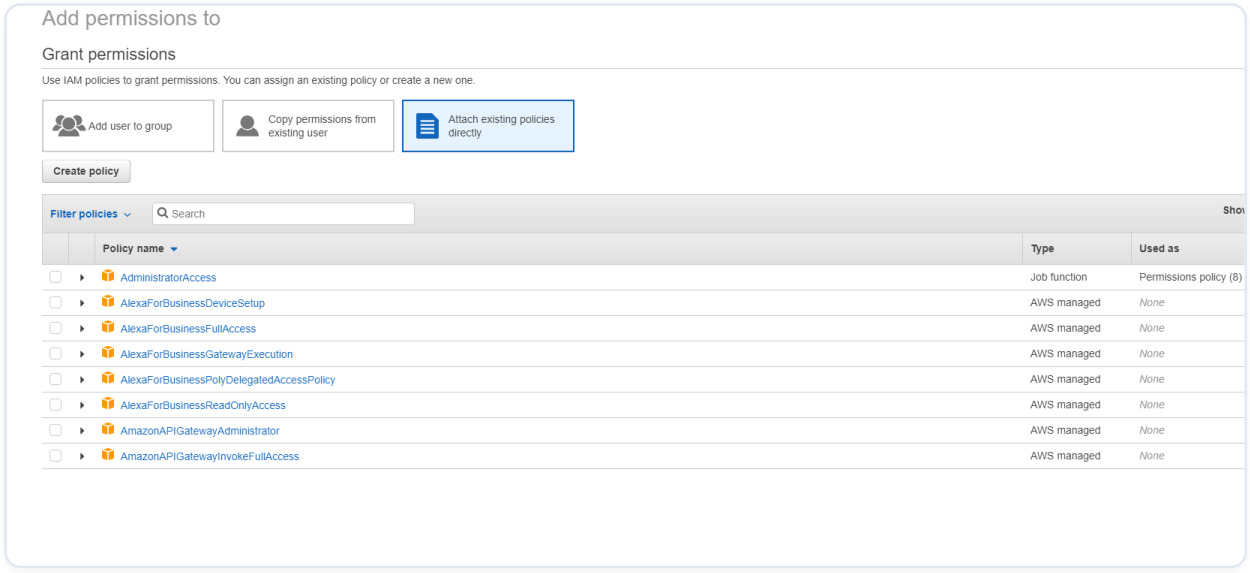
Add the permissions in the **IAM** section of the AWS Management Console:

1. In the **Summary** panel, select the **Permissions** tab.
2. Select **Add permissions.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

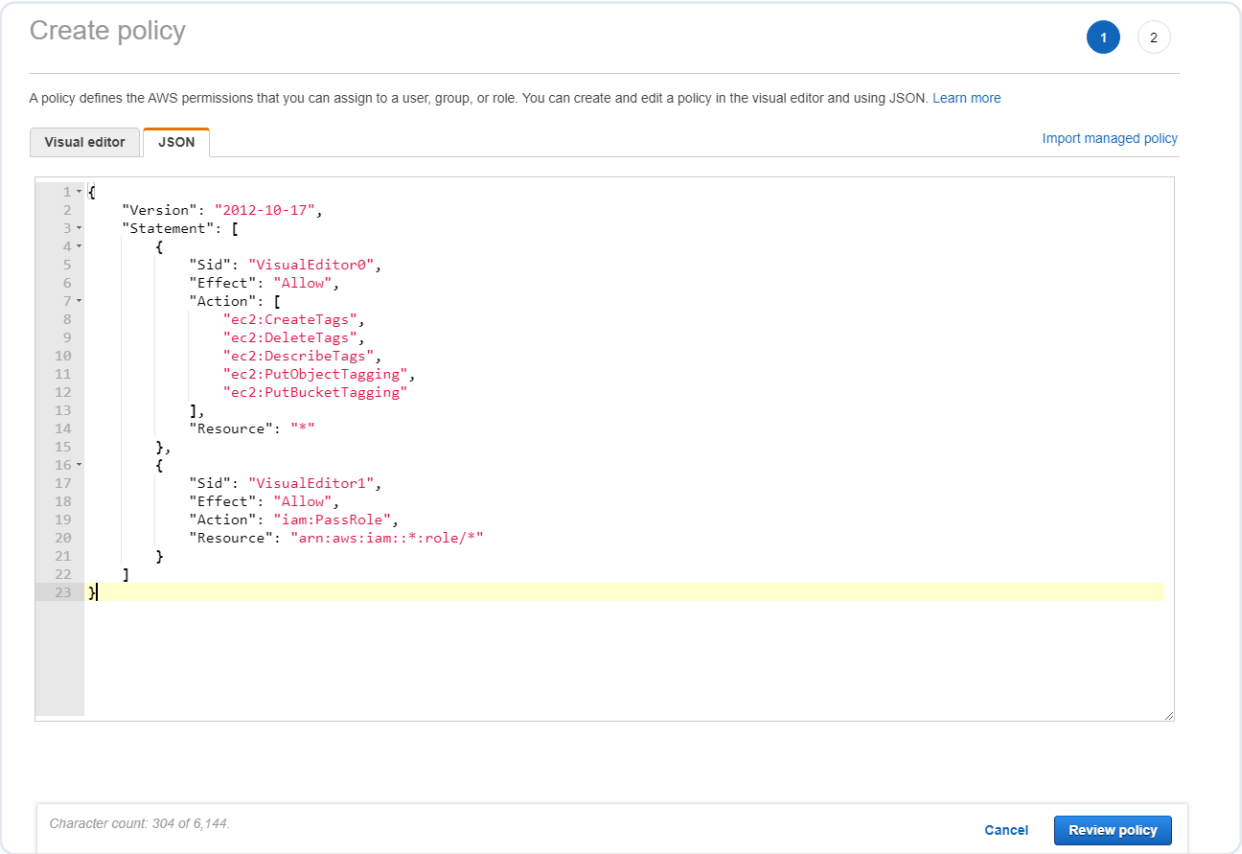


3. In the **Add Permissions to** screen, grant permissions:



4. In the JSON section, include Required AWS permissions for your environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create a connection

You can create a connection to Amazon EC2 using:

- Studio
- PowerShell commands

NOTE:

Check your proxy server or firewall restrictions and ensure that the following address is contactable: `https://*.amazonaws.com`. Also, make sure that all the addresses mentioned in Citrix Gateway service connectivity are contactable.

If these are not contactable, it might cause failure while creating or updating the host connection.

Create a connection using Studio

1. Navigate to **Hosting > Add Connection and Resources** page.
2. On the **Connection** page, follow these steps to configure the connection:
   a. Select **Create a new connection**.
   b. In **Zone**, select the resource location you have set up for your AWS environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Select **Amazon EC2** as the connection type.

d. Select one of the methods to provision the resources:

- If you select **Use this AWS account to provision resources**, then select **Use IAM user access key** or **Use IAM role**. For the IAM user access key, provide your **API key** and **Secret key** for the IAM user that has proper IAM permissions policy for Citrix to manage resources in your AWS account. For the IAM role, make sure that you've assigned an IAM role to the Citrix Cloud Connector instance with proper IAM permissions policy for Citrix to manage resources in your AWS account. See Role-based authentication guide for more information.
- If you select **Use cross-account access to provision resources**, then provide the **ARN** of the IAM role in Account B that the Cloud Connectors (or Delivery Controllers) in Account A must assume and perform provisioning operations in.

e. Enter a connection name and click **Next**.

3. On the **Virtual Machine Location** page, specify the location where the VMs must be provisioned. Select the cloud region, VPC, and availability zone or local zone for creating new VMs.
4. On the **Network** page:

   a. Enter a name for the resources that you selected previously in the availability zone or local zone.

   b. Select one or more subnets in the VPC that you configured in the previous menu.

5. Click through the remaining pages till the **Summary** page.
6. Click **Finish** to create the host connection to Amazon EC2.

IMPORTANT CONSIDERATIONS

When you create a connection using Studio:

- Define proper IAM permissions for Citrix to manage your AWS resources.
- If you use an IAM user access key for Citrix to manage your AWS resources, you must provide the API key and secret key values. You can export the key file containing those values from AWS and then import them. You must also provide the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials.
- If you use an IAM role for Citrix to manage your AWS resources, you must make sure to assign a role with proper IAM permissions to all of your Cloud Connector(s). Role-based authentication guide for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The credentials file for the root AWS account (retrieved from the AWS console) is not formatted the same as credentials files downloaded for standard AWS users. Therefore, Citrix DaaS cannot use the file to populate the API key and secret key fields. Ensure that you are using AWS Identity Access Management (IAM) credentials files.
- The zone can be an availability zone or local zone.

Create a connection using PowerShell

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run the following commands. Following is an example:

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"

$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType "<name of
the connection>" -HypervisorAddress " "@("https://ec2.cn-
north-1.amazonaws.com.cn") -Persist -Scope @() -UserName $apiKey
-SecurePassword $secureKey -ZoneUid $zoneUid



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"

$availabilityZonePath = @($rootPath + $availabilityzone +
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

NOTE:

To create a connection using Role-Based Authentication, specify apiKey and apiSecret as `role_based_auth`.

Limitation

If you change the name of an AWS Virtual Private Cloud (VPC) in the AWS console, then the existing hosting unit in Citrix Cloud™ breaks. When the hosting unit is broken, you cannot create catalogs or add machines to existing catalogs. To resolve the issue, change the name of the AWS VPC back to the original name.

Enhanced proxy configuration for AWS host connection

AWS host connection can read the WinHTTP system proxy value that is configured during Cloud Connector installation if you set the custom property

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`UseSystemProxyForHypervisorTrafficOnConnectors` to `true` when creating or updating a host connection using PowerShell.

Advantages

- Simplifies proxy configuration for AWS host connections.
- Reduces the need for manual PowerShell configuration of server and port values.
- Ensures consistent proxy usage between the Cloud Connector and host connections.
- Improves the success rate of API calls that require proxy access.
- Decreases support requests related to proxy configuration.

Prerequisite

Before setting the custom property while creating the host connection using PowerShell, make sure that you configure the WinHTTP proxy on the Cloud Connector.

Create a new connection with automatic proxy

1. Open PowerShell.
2. Add the Citrix snap-ins:

```
Add-PSSnapin citrix*
```

3. Define the variables for the connection.

```
$hypType = "AWS"



################################################################################
#############

The following items need to be set based on the installed environment

$customProperties is set to enable using the system proxy

$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" /></
CustomProperties>'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$awsEndPoint is set to the desired region for the connection

$awsEndPoint = "https://ec2.us-east-1.amazonaws.com"

$hypConnName is set to the connection name to use

$hypConnName = "ctx-test"

$apiKey is set to the AWS API Key ID or "role_based_auth" if the Cloud
Connector instance has an appropriate role

$apiKey = "role_based_auth"

$secretKey is set to the AWS API Key Secret or "role_based_auth" if the
Cloud Connector instance has an appropriate role

$secretKey = "role_based_auth"

$resourceLocation is set to the connector resource location name

$resourceLocation = "ctx-test"

################################################################################
##############
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$secureSecretKey = ConvertTo-SecureString -String $secretKey
-AsPlainText -Force

$zoneUid = (Get-ConfigZone|Where-Object Name -EQ
"$resourceLocation").Uid
```

NOTE:

Ensure you replace the placeholder values in the `$customProperties`, `$awsEndPoint`, `$hypConnName`, `$apiKey`, `$secretKey`, and `$resourceLocation` variables with the appropriate values for your environment.

4. Create the hypervisor connection.

```
$hypHc = New-Item -Path xdhyp:\Connections `

-Name $hypConnName `

-HypervisorAddress $awsEndPoint `

-UserName $apiKey `

-SecurePassword $secureSecretKey `

-ConnectionType $hypType `

-CustomProperties $customProperties `

-Persist `

-ZoneUid $zoneUid
```

5. Create the Broker hypervisor connection.

```
$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Also, see Update an existing host connection with automatic proxy

Cross-account provisioning

There are use-cases where the Cloud Connectors would like to be placed in a separate AWS account (shared services account or site components account) with IAM roles that have cross-account access (cross-account IAM role) and MCS-provisioned machine catalogs in separate secondary AWS account (workloads accounts), without the need for additional Cloud Connectors in the separate accounts. To support such scenarios, this feature uses VPC peering and cross-account access using IAM roles to make provisioning across different AWS accounts possible for enterprises managing multiple AWS accounts.

With VPC peering, you can have your Cloud Connector, and provisioned VMs in different regions or accounts be able to communicate among each other.

With cross-account access using IAM roles, you allow the primary account (Cloud Connector account) to assume an IAM role to access AWS resources in the secondary account (machine catalog VMs).

To allow Cloud Connector to access the resources of the secondary account, create a host connection after assuming the IAM role from the secondary account.

Prerequisites

Set up the following before creating a host connection for cross-account provisioning:

- Set up VPC peering and configure the security groups in both regions or accounts. See Set up VPC peering.
- Delegate cross-account access using IAM roles. See Delegate cross-account access using IAM role.

Set up VPC peering

Let's assume that VPC A is in the primary account (Account A) and it has the Cloud Connectors and Active Directory. VPC B is in the secondary account (Account B) where you want to provision the VMs.

To set up a VPC peering connection between Account A and Account B, do the following:

1. Create a VPC peering connection. See:
    - Different account same region
    - Different account different region

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Go to your VPC A and to the route table that is associated with the public subnet.
3. Click **Edit Routes > Add route**. Add VPC B's CIDR block in the **Destination** column and add the VPC peering you created in the **Target** column.
4. Repeat Steps 2 and 3, but with the private subnets for VPC A and VPC B (add VPC A's CIDR block). See Update your route tables for a VPC peering connection.
5. Go to the private security group associated with VPC A.
6. Select **Actions**, then **Edit inbound rules**.
7. Select **Add rule**. For type, select **All Traffic**, then in the **Source Column** add:
    - If it is a different region, add VPC B's CIDR Block.
    - If it is a different account but the same region, add the account ID and private security group ID of VPC B separated by a forward slash (Example, 123456789012/sg-1a2b3c4d)
8. Repeat Steps 5 through 7, but with the private security group for VPC B (but add VPC A's CIDR Block or VPC A's account ID and private security group ID of the same region, but different account). See Update your security groups to reference peer security groups.

NOTE:

There is no charge to create a VPC peering connection. However, while VPC peering within an Availability Zone is free, charges apply when data transfer over a VPC peering connection occurs across multiple Availability Zones and regions. See Pricing for a VPC peering connection.

Delegate cross-account access using IAM roles

After setting up VPC peering across accounts, you delegate cross-account access using IAM roles.

With cross-account access using IAM roles, you allow the primary account (Cloud Connector account) to assume an IAM role to access AWS resources in the secondary account (machine catalog VMs).

To access cross-account resources, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMEMBER:

Assumed, VPC A is in the primary account (Account A) and it has the Cloud Connector and Active Directory. VPC B is in the secondary account (Account B) where you want to provision the VMs

1. Set up VPC peering across accounts with the steps mentioned before.
2. Create an IAM role and policy in Account B with minimal Citrix IAM Permissions. See IAM tutorial: Delegate access across AWS accounts using IAM roles. Let's say the arn of this role is "arn:aws:iam::5678:role/citrix-role".
3. Add the Trust policy to the role "arn:aws:iam::5678:role/citrix-role" so that it's allowed to be accessed by Account A role "arn:aws:iam::1234:role/primary-account-citrix-role" as per - Cross account resource access in IAM.
4. Create the IAM role and policy in Account A with the name mentioned before "primary-account-citrix role", which can assume the IAM role and pass the IAM role from the Account B (arn:aws:iam::5678:role/citrix-role).
5. Assign the role "arn:aws:iam::1234:role/primary-account-citrix-role" to all the Cloud Connectors in Account A.

Cloud Connectors can now assume the role from Account B ("arn:aws:iam::5678:role/citrix-role").

Create host connection for cross-account provisioning

Create a host connection in the secondary account (Account B) where you want to provision the VMs. This allows Cloud Connectors of Account A to access the resources in Account B after assuming the role from Account B.

Use PowerShell commands to create the host connection and add the following two custom properties:

- `CrossAccountRoleArn`: If you don't provide `CrossAccountRoleArn` property, then the regular Host Connection is created. In this case, `MaximumAssumeRoleDurationInSeconds` is ignored even if it is provided.
- `MaximumAssumeRoleDurationInSeconds`: `DurationInSeconds` must be between 900 seconds to 3600 seconds. The default is 900 seconds. If you provide a value provided more than 3600, then `DurationInSeconds` is set to 3600.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"

$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)

$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'



$connection = New-Item -Path $connectionPath -ConnectionType "AWS"
-HypervisorAddress "https://ec2.$($cloudRegion).amazonaws.com" -Persist
-Scope @() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

After the host connection is created, create hosting units using Studio or PowerShell. However, select VPC and Networks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Edit a connection

You can edit an existing host connection to:

- Modify the option to provide IAM permissions for Citrix to manage resources
- Modify the maximum number of simultaneous actions (or concurrent machines) per hosting connection
- Modify the scope.
- Configure the maximum number of security groups allowed per elastic network interface (ENI) using PowerShell command
- Update an existing host connection with automatic proxy

Edit options to provide IAM permissions

1. Right-click an existing Amazon EC2 connection.
2. On the **Connection Properties** page, click **Edit settings**.
3. Select one of the options to provide IAM permissions for Citrix to manage resources. Enter the required details and click **Save**.

Modify the maximum number of simultaneous actions

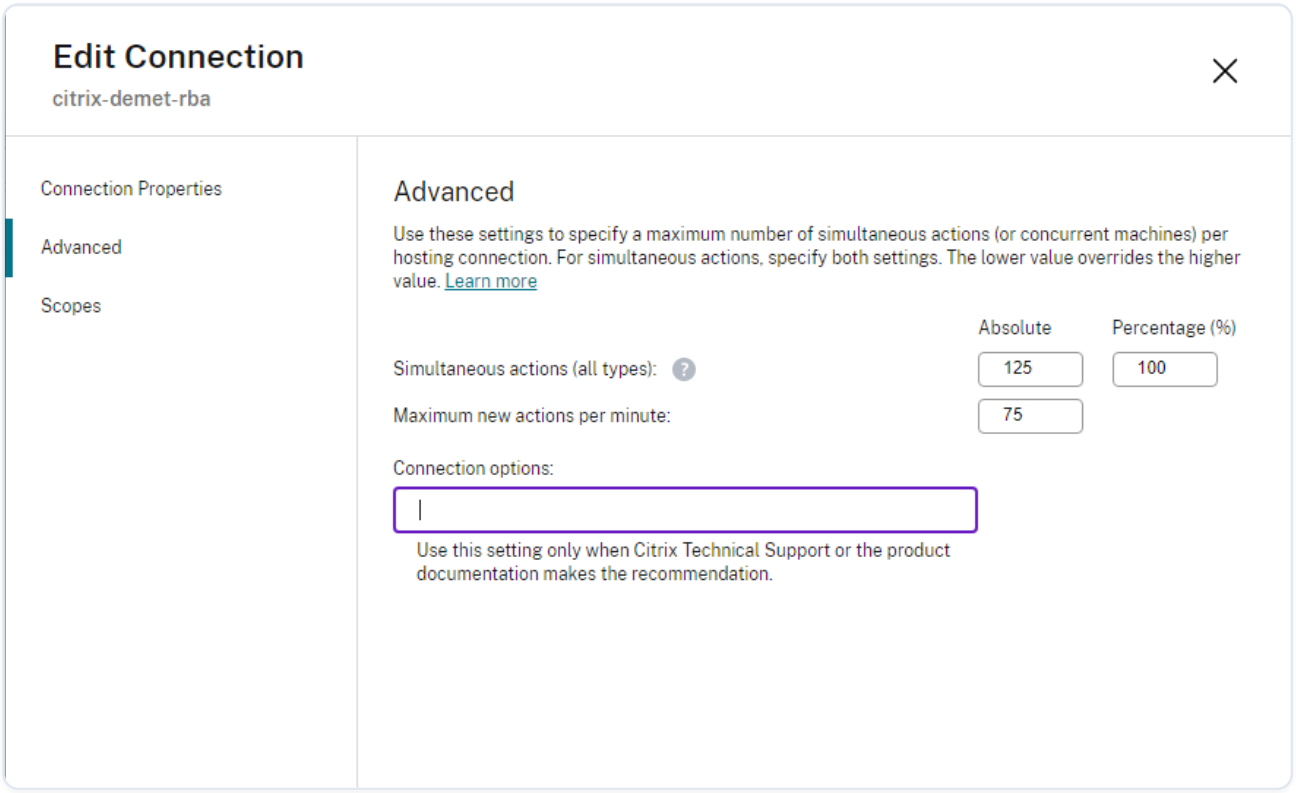
When you create host connections in Studio for Amazon EC2, the following default values display:

OPTION	ABSOLUTE	PERCENTAGE
Simultaneous actions (all types)	125	100
Maximum new actions per minute	150	n/a
Maximum concurrent provisioning operations	100	n/a

MCS supports 100 maximum concurrent provisioning operations by default.

Configure these values by accessing the Citrix Studio **Advanced** section on the **Edit Connection** screen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Alternatively, you can use the Remote PowerShell SDK to set the maximum number of concurrent operations for optimal settings per your environment.

Use the PowerShell custom property, `MaximumConcurrentProvisioningOperations`, to specify the maximum number of concurrent AWS provisioning operations.

Before configuration:

- Ensure you have installed the PowerShell SDK for Cloud.
- Understand that the default value for `MaximumConcurrentProvisioningOperations` is 100.

Perform the following steps to customize the `MaximumConcurrentProvisioningOperations` value:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Enter `cd xdhyp:\Connections\`.
4. Enter `dir` to list the connections.
5. Change or Initialize the Custom Properties string:
    - If the Custom Properties string has a value, copy the Custom Properties into Notepad. Next, change the `MaximumConcurrentProvisioningOperations` property to your preferred value. You can enter a value ranging 1–1000. For example, `<Property`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`.

- If the Custom Properties string is empty or null, you must initialize the string by entering the proper syntax for both the schema and the `MaximumConcurrentProvisioningOperations` property.

6. In the **PowerShell** window, paste the modified Custom Properties from Notepad and assign a variable to the modified Custom Properties. If you initialized the Custom Properties, add the following lines after the syntax:

   `$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="100"/></CustomProperties>'`.

   This string sets the `MaximumConcurrentProvisioningOperations` property to 100. In the Custom Properties string, you must set the `MaximumConcurrentProvisioningOperations` property to a value that aligns with your needs.

7. Enter `Get-XDAuthentication`, which prompts you for your credentials.
8. Run `$cred = Get-Credential`, which might prompt you for solely a Password (or a Name and Password). You might also be prompted for the application ID and associated secret. For connections using role-based authentication, **role_based_auth** is both the Name and Password. Otherwise, enter the AWS API ID and secret.
9. Run `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. You must set the *<connection-name>* to the name of the connection.
10. Enter `dir` to verify the updated CustomProperties string.

Configure security groups per network interface

When editing a host connection, you can now configure the maximum number of security groups allowed per elastic network interface (ENI) using a PowerShell command. For information on AWS security groups quota values, see Security groups.

To configure security groups per network interface:

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Run `cd xdhyp:\Connections\`.
4. Run `dir` to list the connections.
5. Run the following PowerShell command to configure security groups per network interface:

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name
"Citrix_MachineManagement_Options" -Value "
AwsMaxENISecurityGroupLimit=<number>"
```

NOTE:

If you do not set a value for `AwsMaxENISecurityGroupLimit`, then it takes the default value of 5.

Update an existing host connection with automatic proxy

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Enter `cd xdhyp:\Connections\`.
4. Enter `dir` to list the connections.
5. Copy the CustomProperties to a notepad and append property setting `<Property xsi:type="StringProperty" Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True"`.
6. In the **PowerShell** window, paste the modified Custom Properties from Notepad and assign a variable to the modified Custom Properties.
7. Enter `Get-XDAuthentication`, which prompts you for your credentials.
8. Run `$cred = Get-Credential`, which might prompt you for solely a Password (or a Name and Password). You might also be prompted for the application ID and associated secret. For connections using role-based authentication, **role_based_auth** is both the Name and Password. Otherwise, enter the AWS API ID and secret.
9. Run `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. You must set the \<*connection-name*\> to the name of the connection.
10. Enter `dir` to verify the updated CustomProperties string.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service endpoint URL

Standard zone service endpoint URL

When you use MCS, a new AWS connection is added with an API key and an API secret. With this information, along with the authenticated account, MCS queries AWS for the supported zones using the AWS DescribeRegions EC2 API call. The query is made using a generic EC2 Service Endpoint URL `https://ec2.amazonaws.com/`. Use MCS to select the zone for the connection from the list of supported zones. The preferred AWS service endpoint URL is automatically selected for the zone. However, after you create the service endpoint URL, you can no longer set or modify the URL.

Non-standard service endpoint URL

There can be situations where you might not need the automatically chosen AWS Service Endpoint URL for the connection. For such cases, you can use Citrix Cloud SDK and PowerShell to create a connection with a non-standard service endpoint URL. For example, to create a connection using the service endpoint URL `https://ec2.cn-north-1.amazonaws.com.cn`:

1. Set up the AWS hosted Cloud Connector and ensure that it has connectivity.
2. Run the following PowerShell commands to see the list of Cloud Connectors.

```
PS C:\> asnp citrix.*

PS C:\> Get-XDAuthentication

PS C:\> Get-ConfigEdgeServer
```

3. Find the ZoneUid from the newly created Cloud Connector and enter it into the following PowerShell commands. Replace the italicized items with the respective values.

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUid`*ZoneUid*`-
Name`*"My New Connection”*`-ConnectionType "AWS" -HypervisorAddress
@("https://ec2.cn-north-1.amazonaws.com.cn") -UserName`*"APIkey"* `-
Password`*“API Secret”* `-Persist`

`PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hyp. HypervisorConnectionUid
```

4. Refresh the **Hosting** tab to verify that the EC2 connection has been created.
5. Add a resource location using the new connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Required AWS permissions

This section contains the complete list of AWS permissions. Use the complete set of permissions as given in the section for the functionality to work correctly.

NOTE:

The `iam:PassRole` permission is needed only for **role_based_auth**.

Creating a host connection

A new host connection is added using the information obtained from AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Power management of VMs

VMs are powered on or off.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeInstances",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:RebootInstances",

                "ec2:DescribeInstanceStatus"

            ],

            "Effect": "Allow",

            "Resource": "*"

        }

    ]

}
```

Creating, updating, or deleting VMs

A machine catalog is created, updated, or deleted with VMs provisioned as AWS instances.

```
{

    "Version": "2012-10-17",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        }

    ]

}
```

NOTE:

- The EC2 section related to SecurityGroups is only needed if an Isolation Security Group must be created for the Preparation VM during catalog creation. Once this is done, these permissions are not required.

Importing VMs

A machine catalog is created by importing VMs.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeInstances",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeSubnets",

                "ec2:DescribeVolumes",

                "ec2:DescribeSpotInstanceRequests"

            ],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

NOTE:

The `ec2:DescribeSpotInstanceRequests` is needed only if there is a spot instance in the AWS region from where VMs are going to be imported.

DIRECT DISK UPLOAD AND DOWNLOAD

Direct disk upload eliminates the volume worker requirement for machine catalog provisioning, and instead uses public APIs provided by AWS. This functionality reduces the cost associated with extra storage accounts and the complexity for maintaining volume worker operations.

NOTE:

The support for volume worker is removed. The direct disk upload and download permissions are required for machine catalog provisioning.

The following permissions must be added to the policy:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `ec2:DescribeLaunchTemplates`

IMPORTANT:

- You can add a new VM to existing machine catalogs without any volume worker resources such as volume worker AMI, and volume worker VM.
- If you delete an existing catalog that used any volume worker before, all artifacts that are volume worker related are deleted.

EBS encryption of created volumes

EBS can auto-encrypt newly created volumes if the AMI is encrypted, or EBS is configured to encrypt all new volumes. However, to implement the functionality, the following permissions must be included in the IAM policy.

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            ],
            "Resource": "*"
        }
    ]
}
```

NOTE:

The permissions can be limited to specific keys by including a Resource and Condition block at the discretion of the user. For example, **KMS Permissions with Condition**:

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"

            ],

            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true

                }

            }

        }

    ]

}
```

The following key policy statement is the entire default key policy for KMS keys that is required to allow the account to use IAM policies to delegate permission for all actions (kms:*) on the KMS key.

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Resource": ""

}
```

For more information, see the AWS Key Management Service official documentation.

IAM role-based authentication

The following permissions are added to support role-based authentication.

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

Minimal IAM permissions policy

The following JSON can be used for all currently supported features. You can create host connections, create, update, or delete VMs, and do power management using this policy. The policy can be applied to the users as explained in Defining IAM permissions sections or you can also use role-based authentication using **role_based_auth** security key and secret key.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

To use **role_based_auth**, first configure the desired IAM role on the cloud connector ec2 instance when setting up the cloud connector. Using Citrix Studio, add the hosting connection and supply the role_based_auth for the authentication key and secret. A hosting connection with these settings then uses role-based authentication.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "kms:ReEncryptFrom"

            ],

            "Resource": "*"

        },

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

NOTE:

- The EC2 section related to SecurityGroups is only needed if an Isolation Security Group must be created for the Preparation VM during catalog creation. Once this is done, these permissions are not required.
- The KMS section is only required when using EBS volume encryption.
- The `iam:PassRole` permission section is needed only for **role_based_auth**.
- Specific resource-level permissions can be added instead of full access based on your requirements and environment. Refer to AWS documents Demystifying EC2 Resource-Level Permissions and Access management for AWS resources for more details.
- Use `ec2:CreateNetworkInterface` and `ec2:DeleteNetworkInterface` permissions only if you are using the volume worker method.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Validate permissions on host connection

You can validate permissions on a host connection to do tasks related to creating and managing MCS machine catalogs. This implementation helps you to find out the missing permissions required for different scenarios such as creating, deleting, and updating VMs, power management of VMs, and EBS encryption, ahead of time so that you can avoid being blocked at critical times.

You can validate the permissions on a host connection using the PowerShell command `Test-HypHypervisorConnection`. The result from the command is captured as a list where each item in the list is broken into three sections.

- Category: The action or task a user can do to create and manage an MCS machine catalog.
- Corrective Action: The step an admin must do to resolve a users' missing permissions discrepancy.
- Missing permission: The list of missing permissions for a category.

To validate the permissions, do the following:

1. Create a host connection to AWS.
2. Open a PowerShell window from the Delivery Controller™ host.
3. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
4. Run the following command to verify if you have the required permissions to look up your permissions.

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AWSCon"
   ```

5. After you add the missing permissions required to look up your permissions, run the following command to verify if you have permissions in the following categories:

   - Create Update delete
   - Power Management
   - EBS encryption

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:
   \Connections\AWSCon" [-SecurePassword -Password] "password" -UserName
   "" -CustomProperties ""
   ```

For more information on adding permissions, see Add IAM permissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For AWS specific information, see Create an AWS EC2 catalog.

More information

- Create and manage connections and resources
- AWS virtualization environments

Connection to Amazon WorkSpaces Core Managed Instances

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Amazon WorkSpaces Core Managed Instances.

Prerequisites

Do the following before creating a connection to Amazon WorkSpaces Core Managed Instances:

- Complete setting up your AWS as a resource location. See AWS virtualization environments.
- Define IAM permissions policy of IAM user or role for Citrix® to manage AWS resources on your behalf.
- Create a service-linked role.

Define IAM permissions

Before creating a host connection, an IAM permissions policy needs to be properly defined for an IAM user or role that gives Citrix proper permissions to provision and manage resources in your AWS account on your behalf. Use the information in this section to define IAM permissions for Citrix DaaS on Amazon WorkSpaces Core Managed Instances. Amazon's IAM service permits accounts having multiple users, which can be further organized into groups. These users can possess different permissions to control their ability to perform operations associated with the account. For more information about IAM permissions, see the IAM JSON policy reference.

NOTE:

Since Citrix provisions and manages resources and automation in your AWS account on your behalf, configuring IAM permissions policies based on specific tags or resource naming conventions is not supported.

To apply IAM permissions policy to a new group of users:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Log in to the AWS management console and select the **IAM service** from the drop-down list.
2. Select **Create a New Group of Users**.
3. Type a name for the new user group and select **Continue**.
4. On the **Permissions** page, choose **Custom Policy**.
5. Type a name for the **Permissions policy**.
6. In the **Policy Document** section, enter the relevant permissions.

After entering the policy information, select **Continue** to complete the application of the IAM permissions policy to the group of users. Users in the group are granted permissions to do only those actions that are required for Citrix DaaS.

IMPORTANT:

Use the policy text provided in the example provided in this article to list the actions that a Citrix DaaS uses to perform actions within an AWS account without restricting those actions to specific resources. Citrix recommends that you use the example for testing purposes. For production environments, you might choose to add further restrictions on resources.

Add IAM permissions

Add the permissions in the **IAM** section of the AWS Management Console:

1. In the **Summary** panel, select the **Permissions** tab.
2. Select **Add permissions.**
3. In the **Add Permissions to** screen, grant permissions.
4. In the JSON section, include Required AWS permissions for your environment.

Create a service-linked role

For each of your AWS accounts from which Citrix will call Core V2 APIs, create a service-linked role (SLR).

The steps to create the role:

- Open a Command Line Interface (CLI) in the AWS management console.
- Run the following command in the CLI:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
aws iam create-service-linked-role --aws-service-name workspaces-
instances.amazonaws.com
```

You can also configure the service-linked role using the using the Amazon WorkSpaces Core management console. See Creating a service-linked role (console).

Create a connection

You can create a connection to Amazon WorkSpaces Core Managed Instances using:

- Studio
- PowerShell commands

NOTE:

Check your proxy server or firewall restrictions and ensure that the following addresses are contactable: `https://*.amazonaws.com` and `https://*.api.aws`. Also, make sure that all the addresses mentioned in Citrix Gateway service connectivity are contactable.

If these are not contactable, it might cause failure while creating or updating the host connection.

Create a connection using Studio

1. Navigate to **Hosting > Add Connection and Resources** page.
2. On the **Connection** page, follow these steps to configure the connection:
    a. Select **Create a new connection**.
    b. In **Zone**, select the resource location you have set up for your AWS environment.
    c. Select **Amazon WorkSpaces Core** as the connection type.
    d. Select **Use IAM user access key** or **Use IAM role**.

    For the IAM user access key, provide your **API key** and **Secret key** for the IAM user that has proper IAM permissions policy for Citrix to manage resources in your AWS account.

    For the IAM role, make sure that you've assigned an IAM role to the Citrix Cloud Connector instance with proper IAM permissions policy for Citrix to manage resources in your AWS account. See Role-based authentication guide for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. To route API requests to AWS through Citrix Cloud Connectors, select the **Use the system proxy on Citrix Cloud Connectors** checkbox. This ensures that AWS connectivity works properly when Cloud Connectors have no direct Internet access.

f. Enter a connection name and click **Next**.

3. On the **Virtual Machine Location** page, specify the location where the VMs must be provisioned. Select the cloud region, VPC, and availability zone (or local zone) for creating new VMs.
4. On the **Network** page:

   a. Enter a name for the resources that you selected previously in the availability zone (or local zone).

   b. Select one or more subnets in the VPC that you configured in the previous menu.

5. Click through the remaining pages till the **Summary** page.
6. Click **Finish** to create the host connection to Amazon WorkSpaces Core Managed Instances.

IMPORTANT CONSIDERATIONS

When you create a connection using Studio:

- Define proper IAM permissions for Citrix to manage your AWS resources.
- If you use an IAM user access key for Citrix to manage your AWS resources, you must provide the API key and secret key values. You can export the key file containing those values from AWS and then import them. You must also provide the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials.
- If you use an IAM role for Citrix to manage your AWS resources, you must make sure to assign a role with proper IAM permissions to all of your Cloud Connector(s). Role-based authentication guide for more information.
- The credentials file for the root AWS account (retrieved from the AWS console) is not formatted the same as credentials files downloaded for standard AWS users. Therefore, Citrix DaaS cannot use the file to populate the API key and secret key fields. Ensure that you are using AWS Identity Access Management (IAM) credentials files.
- The zone can be an availability zone or local zone.

Create a connection using PowerShell

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Run the following commands. Following is an example:

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"

$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType
"AmazonWorkSpacesCoreMachineManagerFactory" -HypervisorAddress "
"https://workspaces-instances.$($cloudRegion).api.aws"" -Persist -Scope
@() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"

$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"

$availabilityZonePath = @($rootPath + $availabilityzone +
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

NOTE:

To create a connection using Role-Based Authentication, specify apiKey and apiSecret as `role_based_auth`.

Limitation

If you change the name of an AWS Virtual Private Cloud (VPC) in the AWS console, then the existing hosting unit in Citrix Cloud™ breaks. When the hosting unit is broken, you cannot create catalogs or add machines to existing catalogs. To resolve the issue, change the name of the AWS VPC back to the original name.

Create a secure environment for AWS-managed traffic

If you have a proxy configured on the Cloud Connectors, then you must create the host connection to use the proxy so that API calls made by MCS are properly routed through the proxy. MCS enables network traffic (API calls from Citrix Cloud to AWS hypervisor) to be routed through Cloud Connectors in your environment.

The host connection can read the WinHTTP system proxy value that is configured during Cloud Connector installation. You can configure the proxy using Studio or by setting the custom property `UseSystemProxyForHypervisorTrafficOnConnectors` to `True` when creating or updating a host connection using PowerShell.

NOTE:

If your environment uses a proxy, ensure that SSL inspection is disabled or SSL connection remains unaltered for `<https://workspaces-instances.*.api.aws/>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CREATE A HOST CONNECTION CONFIGURED WITH THE PROXY

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run the PowerShell commands to configure the proxy. For example:

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$zoneUid = "00000000-0000-0000-0000-000000000000"



$securePassword = Read-Host 'Please enter your secret key'
-AsSecureString

$connectionPath = "XDHyp:\Connections\" + $connectionName



$customProperties = @"

<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />

</CustomProperties>

"@
```

4. Create a hosting connection. For example:

```
$connection = New-Item -Path $connectionPath `

-ConnectionType "Custom" -PluginId
"AmazonWorkSpacesCoreMachineManagerFactory" `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-HypervisorAddress "https://workspaces-instances.$
($cloudRegion).api.aws" `

-CustomProperties> $customProperties `

-Persist -Scope @()`

-UserName $apiKey -SecurePassword $securePassword `

-ZoneUid $zoneUid



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

To enable the proxy for an existing host connection, see Enable the proxy on an existing connection.

Cross-account provisioning

There are use-cases where the Cloud Connectors would like to be placed in a separate AWS account (shared services account or site components account) with IAM roles that have cross-account access (cross-account IAM role) and MCS-provisioned machine catalogs in separate secondary AWS account (workloads accounts), without the need for additional Cloud Connectors in the separate accounts. To support such scenarios, this feature uses VPC peering and cross-account access using IAM roles to make provisioning across different AWS accounts possible for enterprises managing multiple AWS accounts.

With VPC peering, you can have your Cloud Connector, and provisioned VMs in different regions or accounts be able to communicate among each other.

With cross-account access using IAM roles, you allow the primary account (Cloud Connector account) to assume an IAM role to access AWS resources in the secondary account (machine catalog VMs).

To allow Cloud Connector to access the resources of the secondary account, create a host connection after assuming the IAM role from the secondary account.

Prerequisites

Set up the following before creating a host connection for cross-account provisioning:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Set up VPC peering and configure the security groups in both regions or accounts. See Set up VPC peering.
- Delegate cross-account access using IAM roles. See Delegate cross-account access using IAM role.

Set up VPC peering

Let's assume that VPC A is in the primary account (Account A) and it has the Cloud Connectors and Active Directory. VPC B is in the secondary account (Account B) where you want to provision the VMs.

To set up a VPC peering connection between Account A and Account B, do the following:

1. Create a VPC peering connection. See:
    - Different account same region
    - Different account different region
2. Go to your VPC A and to the route table that is associated with the public subnet.
3. Click **Edit Routes > Add route**. Add VPC B's CIDR block in the **Destination** column and add the VPC peering you created in the **Target** column.
4. Repeat Steps 2 and 3, but with the private subnets for VPC A and VPC B (add VPC A's CIDR block). See Update your route tables for a VPC peering connection.
5. Go to the private security group associated with VPC A.
6. Select **Actions**, then **Edit inbound rules**.
7. Select **Add rule**. For type, select **All Traffic**, then in the **Source Column** add:
    - If it is a different region, add VPC B's CIDR Block.
    - If it is a different account but the same region, add the account ID and private security group ID of VPC B separated by a forward slash (Example, 123456789012/sg-1a2b3c4d)
8. Repeat Steps 5 through 7, but with the private security group for VPC B (but add VPC A's CIDR Block or VPC A's account ID and private security group ID of the same region, but different account). See Update your security groups to reference peer security groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

There is no charge to create a VPC peering connection. However, while VPC peering within an availability zone is free, charges apply when data transfer over a VPC peering connection occurs across multiple availability zones and regions. See Pricing for a VPC peering connection.

Delegate cross-account access using IAM roles

After setting up VPC peering across accounts, you delegate cross-account access using IAM roles.

With cross-account access using IAM roles, you allow the primary account (Cloud Connector account) to assume an IAM role to access AWS resources in the secondary account (machine catalog VMs).

To access cross-account resources, do the following:

REMEMBER:

Assumed, VPC A is in the primary account (Account A) and it has the Cloud Connector and Active Directory. VPC B is in the secondary account (Account B) where you want to provision the VMs

1. Set up VPC peering across accounts with the steps mentioned before.
2. Create an IAM role and policy in Account B with minimal Citrix IAM Permissions. See IAM tutorial: Delegate access across AWS accounts using IAM roles. Let's say the arn of this role is "arn:aws:iam::5678:role/citrix-role".
3. Add the Trust policy to the role "arn:aws:iam::5678:role/citrix-role" so that it's allowed to be accessed by Account A role "arn:aws:iam::1234:role/primary-account-citrix-role" as per - Cross account resource access in IAM.
4. Create the IAM role and policy in Account A with the name mentioned before "primary-account-citrix role", which can assume the IAM role and pass the IAM role from the Account B (arn:aws:iam::5678:role/citrix-role).
5. Assign the role "arn:aws:iam::1234:role/primary-account-citrix-role" to all the Cloud Connectors in Account A.

Cloud Connectors can now assume the role from Account B ("arn:aws:iam::5678:role/citrix-role").

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create host connection for cross-account provisioning

Create a host connection in the secondary account (Account B) where you want to provision the VMs. This allows Cloud Connectors of Account A to access the resources in Account B after assuming the role from Account B.

Use PowerShell commands to create the host connection and add the following two custom properties:

- `CrossAccountRoleArn`: If you don't provide `CrossAccountRoleArn` property, then the regular host connection is created. In this case, `MaximumAssumeRoleDurationInSeconds` is ignored even if it is provided.
- `MaximumAssumeRoleDurationInSeconds`: `DurationInSeconds` must be between 900 seconds to 3600 seconds. The default is 900 seconds. If you provide a value provided more than 3600, then `DurationInSeconds` is set to 3600.

Example:

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"

$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)

$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$connection = New-Item -Path $connectionPath -ConnectionType
"AmazonWorkSpacesCoreMachineManagerFactory" -HypervisorAddress "https://
workspaces-instances.$($cloudRegion).api.aws" -Persist -Scope @()
-UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

After the host connection is created, create hosting units using Studio or PowerShell. However, select VPC and Networks.

Bypass Cloud Connectors for AWS API requests

In Amazon WorkSpaces Core Managed Instance (MI) environments, the Citrix Machine Creation Services (MCS) plugin typically resides on the Delivery Controller and routes AWS API requests through the Citrix Cloud Connector via a proxy.

You can configure host connections to bypass the Cloud Connector for AWS API requests. When this feature is enabled, the plugin makes API calls—including those for provisioning and power management—directly from the DDC to AWS services (such as Amazon EC2, EBS, and WorkSpaces Instances), removing the dependency on going through Cloud Connector via a proxy.

Benefits

- Reduce AWS API call dependency on Cloud Connectors: Removing the AWS API dependency on the Cloud Connector is a key step for customers aiming to reduce their on-premises or cloud infrastructure footprint.
- Reduced Resource Consumption: Less traffic through the Cloud Connector reduces the compute requirements for the Connector VM, potentially leading to cost savings.
- Operational Flexibility: Provides higher availability by removing a potential point of failure (the Cloud Connector/NGS proxy path) for critical power management and provisioning tasks.

Limitations and considerations

Before enabling this feature, consider the following requirements and limitations:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Authentication: Role-based authentication (IAM roles) is not supported when bypassing the Cloud Connector. You must configure the setup for IAM user access keys only.
- Environment scope: This feature is exclusive to Amazon WorkSpaces Core Managed Instances (MI). It is not supported for standard AWS EC2 host connections.
- Network requirements: The DDC must have a direct network path to the AWS service endpoints.
- Resource location Health: If a Cloud Connector was originally provisioned in the resource location, it must remain powered on. Non-MCS components and health checks still rely on the Cloud Connector if it exists.
- Unsupported features:
  - Cross-account provisioning
  - System proxy usage
- Connector requirements: While this feature removes the API dependency, there are other configurations needed to reduce dependencies on Cloud Connectors (not that requirements for Cloud Connectors may not be limited to the ones listed here):
  - Domain join: Using Non-Domain Joined or Microsoft Entra hybrid joined machines.
  - VDA registration: Enabling Rendezvous V2 (DDC direct to VDA communication via WebSockets) for VDA registration.

Create a host connection with API bypass

When creating a host connection in Full Configuration (Studio), you can now select Amazon WorkSpaces Core resource locations even if no Cloud Connectors are present in that location.

To enable the bypass via PowerShell, use the `BypassConnectorForAwsApiRequests` custom property.

PowerShell Example:

```
$custProp = '<CustomProperties xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">

  <Property xsi:type="StringProperty"
Name="BypassConnectorForAwsApiRequests" Value="true" />

</CustomProperties>'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$connectionName = "MyWSCConnection"

$cloudRegion = "us-east-1"

$apiKey = "YOUR_IAM_ACCESS_KEY"

$zoneUid = (Get-ConfigZone | Where-Object {$_.Name -eq
"MyResourceLocation"}).Uid

$securePassword = Read-Host 'Enter your IAM Secret Key' -AsSecureString



$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath `

    -ConnectionType "Custom" `

    -PluginId "AmazonWorkSpacesCoreMachineManagerFactory" `

    -HypervisorAddress "https://workspaces-instances.$
($cloudRegion).api.aws" `

    -Persist -Scope @() `

    -CustomProperties $custProp `

    -UserName $apiKey -SecurePassword $securePassword `

    -ZoneUid $zoneUid



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage existing connections

You can enable or disable the bypass feature for existing host connections.

- Enabling on existing connections: You can modify the custom properties of an existing connection to include `BypassConnectorForAwsApiRequests = true.`
- Disabling: If disabled, the DDC resumes routing AWS API calls through the Cloud Connector via the NGS proxy. Note that this requires a functional Cloud Connector and NGS proxy path to be available in the resource location.

Troubleshooting

If you attempt to enable the bypass property under unsupported conditions, the system returns a validation error:

- IAM Roles/Cross-Account/Proxy: If enabled alongside IAM roles, cross-account provisioning, or system proxies, the `New-Item` command fails with:

  ```
  AmazonWorkSpacesCoreException: Bypassing the Cloud Connector For AWS
  API requests is not supported for IAM roles, Cross-Account provisioning
  and System Proxy.
  ```

- Unsupported Connection Type: If applied to a standard Amazon EC2 (AWS) connection, the system fails with:

  ```
  AmazonWorkSpacesCoreException: Bypassing the Cloud Connector For AWS
  API requests is not supported for EC2 host connection.
  ```

Edit a connection

You can edit an existing host connection to:

- Modify the option to provide IAM permissions for Citrix to manage resources
- Modify the maximum number of simultaneous actions (or concurrent machines) per hosting connection
- Modify the scope.
- Configure the maximum number of security groups allowed per elastic network interface (ENI) using PowerShell command
- Enable the proxy to create a secure environment for AWS-managed traffic

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Edit options to provide IAM permissions

1. Right-click an existing Amazon WorkSpaces Core connection.
2. On the **Connection Properties** page, click **Edit settings**.
3. Select one of the options to provide IAM permissions for Citrix to manage resources. Enter the required details and click **Save**.

Modify the maximum number of simultaneous actions

When you create host connections in Studio for Amazon WorkSpaces Core Managed Instances, the following default values display:

OPTION	ABSOLUTE	PERCENTAGE
Simultaneous actions (all types)	125	100
Maximum new actions per minute	150	n/a
Maximum concurrent provisioning operations	150	n/a

MCS supports 150 maximum concurrent provisioning operations by default.

You can configure these values by accessing the Citrix Studio **Advanced** section on the **Edit Connection** screen:

Alternatively, you can use the Remote PowerShell SDK to set the maximum number of concurrent operations for optimal settings per your environment.

Use the PowerShell custom property, `MaximumConcurrentProvisioningOperations`, to specify the maximum number of concurrent AWS provisioning operations.

Before configuration:

- Ensure that you have installed the PowerShell SDK for Cloud.
- Understand that the default value for `MaximumConcurrentProvisioningOperations` is 150.

Perform the following steps to customize the `MaximumConcurrentProvisioningOperations` value:

1. Open a **PowerShell** window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Enter `cd xdhyp:\Connections\`.
4. Enter `dir` to list the connections.
5. Change or Initialize the Custom Properties string:
   - If the Custom Properties string has a value, copy the Custom Properties into Notepad. Next, change the `MaximumConcurrentProvisioningOperations` property to your preferred value. You can enter a value ranging 1–1000. For example, `<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`.
   - If the Custom Properties string is empty or null, you must initialize the string by entering the proper syntax for both the schema and the `MaximumConcurrentProvisioningOperations` property.
6. In the **PowerShell** window, paste the modified Custom Properties from Notepad and assign a variable to the modified Custom Properties. If you initialized the Custom Properties, add the following lines after the syntax:

   ```
   $customProperties = '<CustomProperties xmlns="http://
   schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
   www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'
   ```

   This string sets the `MaximumConcurrentProvisioningOperations` property to 100. In the Custom Properties string, you must set the `MaximumConcurrentProvisioningOperations` property to a value that aligns with your needs.
7. Enter `Get-XDAuthentication`, which prompts you for your credentials.
8. Run `$cred = Get-Credential`, which might prompt you for solely a Password (or a Name and Password). You might also be prompted for the application ID and associated secret. For connections using role-based authentication, **role_based_auth** is both the Name and Password. Otherwise, enter the AWS API ID and secret.
9. Run `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. You must set the *<connection-name>* to the name of the connection.
10. Enter `dir` to verify the updated CustomProperties string.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure security groups per network interface

When editing a host connection, you can now configure the maximum number of security groups allowed per elastic network interface (ENI) using a PowerShell command. For information on AWS security groups quota values, see Security groups.

To configure security groups per network interface:

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run `cd xdhyp:\Connections\`.
4. Run `dir` to list the connections.
5. Run the following PowerShell command to configure security groups per network interface:

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name
"Citrix_MachineManagement_Options" -Value "
AwsMaxENISecurityGroupLimit=<number>"
```

NOTE:

If you do not set a value for `AwsMaxENISecurityGroupLimit`, then it takes the default value of 5.

Enable the proxy on an existing connection

1. Open a PowerShell window.
2. Run the following commands.

```
Add-PSSnapin citrix*.

cd XDHyp:\Connections\

dir
```

3. Copy the `CustomProperties` from the connection to a notepad and append property setting `<Property xsi:type="StringProperty" Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />` to the `CustomProperties` to enable the proxy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. In the PowerShell window, assign a variable to the modified custom properties. For example:

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">

<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />

</CustomProperties>'
```

5. Enter `Get-XDAuthentication`, which prompts you for your credentials.
6. Run `$cred = Get-Credential`, which might prompt you for solely a Password (or a Name and Password). You might also be prompted for the application ID and associated secret. For connections using role-based authentication, `role_based_auth` is both the Name and Password. Otherwise, enter the AWS API ID and secret.
7. Run `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. You must set the `<connection-name>` to the name of the connection.
8. Enter `dir` to verify the updated `CustomProperties` string.

Service endpoint URL

Standard zone service endpoint URL

When you use MCS, a new Amazon WorkSpaces Core Managed Instances connection is added with an API key and an API secret. With this information, along with the authenticated account, MCS queries AWS for the supported regions and zones using AWS EC2 and Amazon WokrSpaces Core Managed Instances API calls. The query is made using a Workspace Instances Service Endpoint URL `<https://workspaces-instances.us-east-1.api.aws/>` and EC2 Service Endpoint https:/ec2.us-east-1.api.aws/.

NOTE:

Make sure that `<https://workspaces-instances.us-east-1.api.aws/>` is contactable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Non-standard service endpoint URL

There can be situations where you might not need the automatically chosen AWS Service Endpoint URL for the connection. For such cases, you can use Citrix Cloud SDK and PowerShell to create a connection with a non-standard service endpoint URL. For example, to create a connection using the service endpoint URL `https://ec2.cn-north-1.amazonaws.com.cn`:

1. Set up the AWS hosted Cloud Connector and ensure that it has connectivity.
2. Run the following PowerShell commands to see the list of Cloud Connectors.

```
PS C:\> asnp citrix.*

PS C:\> Get-XDAuthentication

PS C:\> Get-ConfigEdgeServer
```

3. Find the ZoneUid from the newly created Cloud Connector and enter it into the following PowerShell commands. Replace the italicized items with the respective values.

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUid ZoneUid -Name
“My New Connection” -ConnectionType "Custom" -HypervisorAddress
@("https://workspaces-instances.$($cloudRegion).api.aws")-PluginId
"AmazonWorkSpacesCoreMachineManagerFactory" -UserName “APIkey”
-Password “API Secret” -Persist



PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hyp. HypervisorConnectionUid
```

4. Refresh the **Hosting** tab to verify that the connection has been created.
5. Add a resource location using the new connection.

Required AWS permissions

This section contains the complete list of AWS permissions. Use the complete set of permissions as given in the section for the functionality to work correctly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The `iam:PassRole` permission is needed only for using IAM roles for Citrix to manage resources.

Creating a host connection

A new host connection is added using the information obtained from AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "workspaces-instances:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Power management of VMs

VMs are powered on or off.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeInstances",,

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:RebootInstances",

                "ec2:DescribeInstanceStatus"

            ],

            "Effect": "Allow",

            "Resource": "*"

        },

        {

           "Action": [

               "workspaces-instances:*"

           ],

           "Effect": "Allow",

            "Resource": "*"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        }


    ]


}
```

Creating, updating, or deleting VMs

A machine catalog is created, updated, or deleted with VMs provisioned as AWS instances.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "workspaces-instances:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetAccountSummary",
                "ec2:CopyImage"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            ],
            "Resource": "*"
        },


    ]
}
```

NOTE:

- The EC2 section related to SecurityGroups is only needed if an Isolation Security Group must be created for the Preparation VM during catalog creation. Once this is done, these permissions are not required.
- The EC2 `CopyImage` and IAM `GetAccountSummary` permissions are needed only when sharing prepared images across regions. See Share prepared images across availability zones and regions.

Direct disk upload and download

The following permissions must be added to the policy:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EBS encryption of created volumes

EBS can auto-encrypt newly created volumes if the AMI is encrypted, or EBS is configured to encrypt all new volumes. However, to implement the functionality, the following permissions must be included in the IAM policy.

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The permissions can be limited to specific keys by including a Resource and Condition block at the discretion of the user. For example, **KMS Permissions with Condition**:

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"

            ],

            "Condition": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "Bool": {

                    "kms:GrantIsForAWSResource": true

                }

            }

        }

    ]

}
```

The following key policy statement is the entire default key policy for KMS keys that is required to allow the account to use IAM policies to delegate permission for all actions (kms:*) on the KMS key.

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

For more information, see the AWS Key Management Service official documentation.

IAM role-based authentication

The following permissions are added to support role-based authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

Minimal IAM permissions policy

The following JSON can be used for all currently supported features. You can create host connections, create, update, or delete VMs, and do power management using this policy. The policy can be applied to the users as explained in Define IAM permissions sections or you can also use role-based authentication by selecting **Use IAM role** when configuring a host connection.

IMPORTANT:

To use **IAM roles for Citrix to manage resources**, first configure the desired IAM role on the cloud connector ec2 instance when setting up the cloud connector. Using Citrix Studio, add the hosting connection and select the **Use IAM role** option. A hosting connection with these settings then uses role-based authentication.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-instances:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetAccountSummary",
                "ec2:CopyImage"
            ],
            "Resource": "*"
        }

    ]
}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- The EC2 section related to SecurityGroups is only needed if an Isolation Security Group must be created for the Preparation VM during catalog creation. Once this is done, these permissions are not required.
- The KMS section is only required when using EBS volume encryption.
- The `iam:PassRole` permission section is needed only for using IAM roles for Citrix to manage resources.
- Specific resource-level permissions can be added instead of full access based on your requirements and environment. Refer to AWS documents Demystifying EC2 Resource-Level Permissions and Access management for AWS resources for more details.
- Use `ec2:CreateNetworkInterface` and `ec2:DeleteNetworkInterface` permissions only if you are using the volume worker method.

Where to go next

- For creating prepared images, see Create a prepared image for Amazon WorkSpaces Core Managed Instances

More information

- Create and manage connections and resources
- AWS virtualization environments
- For Amazon WorkSpaces Core GitHub PowerShell examples, see citrix-mcs-sdk-samples-Amazon WorkSpaces Core.

Connection to Google cloud environments

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Google cloud environments.

NOTE:

Before creating a connection to Google cloud environments, you need to first finish setting up your Google cloud account as a resource location. See Google Cloud virtualization environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add a connection

In Studio, follow the guidance in Create and manage connections and resources. The following description guides you through setting up a hosting connection:

1. From Studio, select **Hosting** in the left pane.
2. Select **Add Connection and Resources** in the action bar.
3. On the **Connection** page, select **Create a new Connection** and **Citrix provisioning™ tools**, and then select **Next**.

    - **Zone name**. Select a zone (equivalent to a resource location) where you want your host resources to reside. Zones are created automatically when you create a resource location and add a Cloud Connector to it. For more information, see Zones.
    - **Connection type**. Select **Google Cloud Platform** from the menu.
    - **Service account key**. Import the key contained in your Google credential file (.json). You can either paste the key from the credential file or browse to the credential file. To paste the key:

        a. Locate your credential file

        b. Open the file with Notepad (or any text editor)

        c. Copy the content.

        d. Return to the **Connection** page, select **Add key**, paste the content, and then select **Done**.

    - **Service account ID**. The field automatically populates with the information from the service account key.
    - **Connection name**. Type a name for the connection.
    - **Route traffic through Citrix Cloud Connectors**. To route the API requests through an available Citrix Cloud Connector™, select this checkbox. When Cloud Connectors have no direct internet access, you can select **Use the proxy configured on Citrix Cloud Connectors** to ensure GCP connectivity works properly through Citrix Cloud Connectors. You can also select **Enable Google Cloud Build to use private pools** checkbox for an additional layer of security.

        Alternatively, you can enable this feature using PowerShell. For more information, see Create a secure environment for GCP-managed traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

This option is available only when there are active Citrix Cloud™ Connectors in your deployment. Currently, this feature is not supported for Connector Appliances.

- **Create virtual machines using**. Select a method to create virtual machines.

4. On the **Region** page, select a project name from the menu, select a region containing the resources you want to use, and then select **Next**.
5. On the **Network** page, type a name for the resources, select a virtual network from the menu, select a subset, and then select **Next**. The resource name helps identify the region and network combination. Virtual networks with the *(Shared)* suffix appended to their name represent shared VPCs. If you configure a subnet-level IAM role for a shared VPC, only specific subnets of the shared VPC appear on the subnet list.

NOTE:

- The resource name can contain 1–64 characters, and cannot contain only blank spaces or the characters `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`.

6. On the **Summary** page, confirm the information and then select **Finish** to exit the **Add Connection and Resources** window.

After you create the connection and resources, the connection and resources you created are listed. To configure the connection, select the connection and then select the applicable option in the action bar.

Similarly, you can delete, rename, or test the resources created under the connection. To do so, select the resource under the connection and then select the applicable option in the action bar.

Create a secure environment for GCP managed traffic

You can allow only private Google access to your Google Cloud projects. This implementation enhances security to handle sensitive data. To do this:

1. Install Cloud Connectors in the VPC where you want to enforce VPC service controls. See VPC Service Controls for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Add `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` in case of Citrix Cloud deployment. If you are using a private worker pool, add `UsePrivateWorkerPool` in `CustomProperties`. For information on the private worker pool, see Private pools overview.

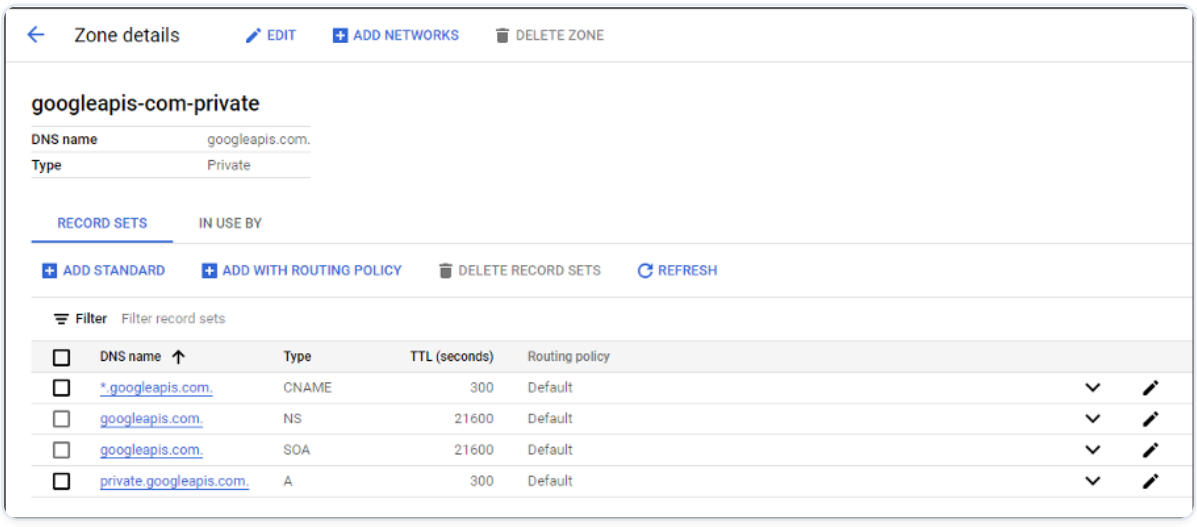
NOTE:

Currently, this feature is not supported for Connector Appliance.

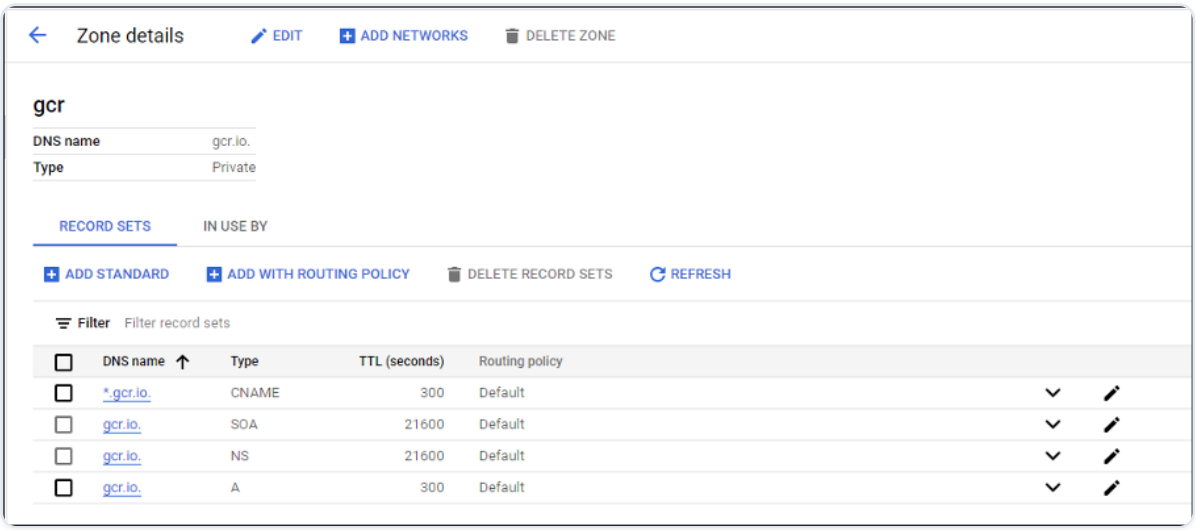
Requirements to create a secure environment for GCP managed traffic

The requirements to create a secure environment for GCP managed traffic are:

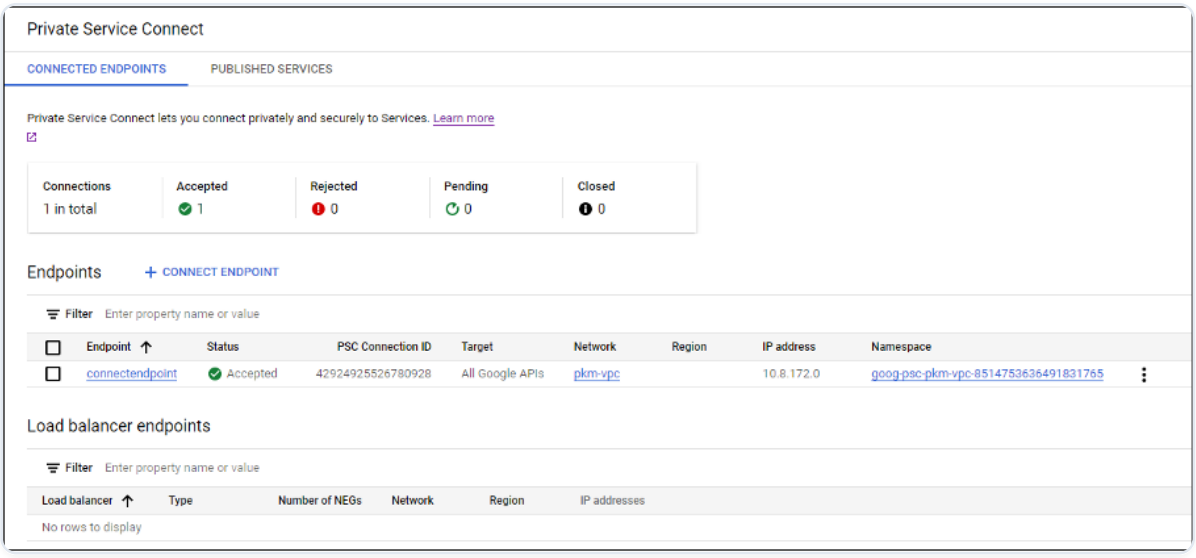
- Ensure that the hosting connection is in maintenance mode when updating the custom properties.
- To use private worker pools, the following changes are required:
  - For Citrix Cloud Service Account, add the following IAM roles:
    - Cloud Build Service Account
    - Compute Instance Admin
    - Service Account User
    - Service Account Token Creator
    - Cloud Build WorkerPool Owner
  - Create the Citrix Cloud Service Account in the same project that you use for creating a hosting connection.
  - Set up DNS zones for `private.googleapis.com` and `gcr.io` as described in DNS configuration.



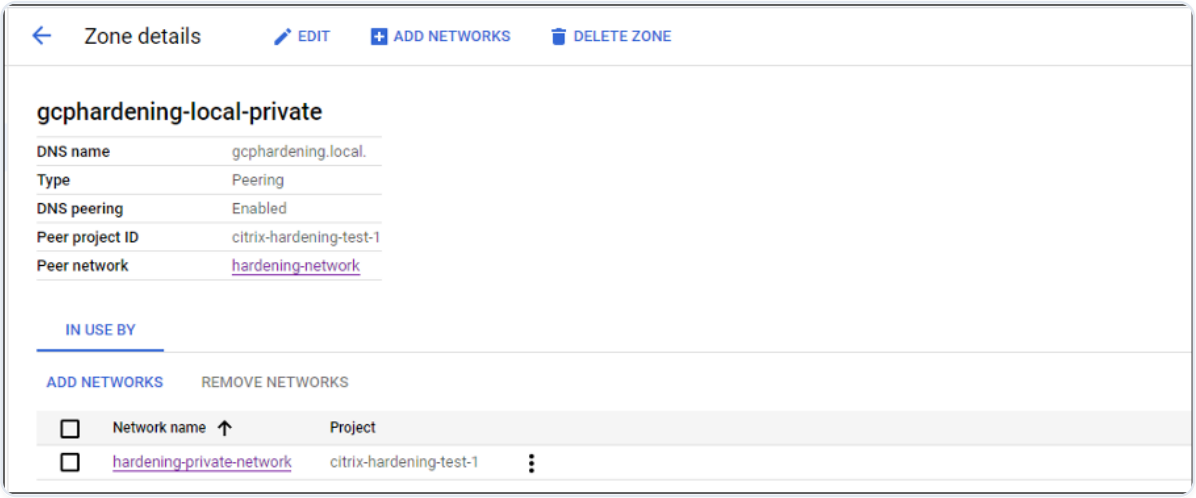
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Set up private Network Address Translation (NAT) or use private service connect. For more information, see Access Google APIs through endpoints.



- If using a peered VPC, create a Cloud DNS zone peering to the peered VPC. For more information, see Create a peering zone.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In VPC service controls, set up Egress rules so that the APIs and VMs can talk to the internet. Ingress rules are optional. For example:

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:

Projects =

All projects

Service =

Service name: All services
```

Enable the proxy

To enable the proxy, set the custom properties as follows on the host connection:

1. Open a PowerShell window from the Delivery Controller host or use the Remote PowerShell SDK. For more information on Remote PowerShell SDK, see SDKs and APIs.
2. Run the following commands:
   a. `Add-PSSnapin citrix*`
   b. `cd XDHyp:\Connections\`
   c. `dir`
3. Copy the `CustomProperties` from the connection to a notepad.
4. Append the property setting as follows:
   - In case of cloud deployment (using public pools): Append property setting `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>` to the `CustomProperties` to enable the proxy. For example:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.citrix.com/2014/xd/machinecreation">
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>

</CustomProperties>
```

Allow ingress rule for Cloud Build Service Account in VPC service perimeter. For example:

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed

To:

Projects =

All projects

Services =

Service name: All services
```

For information on VPC service perimeter, see Service perimeter details and configuration.

- In case of a private worker pool in a cloud deployment, append property setting `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>` and `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>` to the `CustomProperties` to enable the proxy. For example:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

</CustomProperties>
```

5. In the PowerShell window, assign a variable to the modified custom properties. For example: `$customProperty = '<CustomProperties…</CustomProperties>'`.
6. Run `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`.
7. Run `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.
8. Run `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`.
9. Run the following to update an existing host connection:

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION
NAME HERE>') -SecurePassword $securePassword -UserName
$gcpServiceAccount -CustomProperties $customProperty
```

Option to use system proxy on Citrix Cloud Connectors for redirected GCP API traffic

To route all external traffic through a non-transparent proxy, configure the host connection with the custom property `UseSystemProxyForHypervisorTrafficOnConnectors`. This redirects GCP API internet traffic on Citrix Cloud Connectors through the system proxy. Do the same steps as outlined in Enable the proxy to configure the host connection with the custom property. However, make sure to append property setting `<Property xsi:type="StringProperty" Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />` to the `CustomProperties` to enable the proxy.

```
<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />
```

Example:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

 <Property xsi:type="StringProperty"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>

 <Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />

</CustomProperties>
```

NOTE:

After you set this property, the proxy configured in the `netsh winhttp` settings on the Citrix Cloud Connectors is used for outbound traffic to the cloud service provider.

Specify CMEK global and regional key

NOTE:

Support for CMEK in GCP is currently under Preview.

There are two types of customer-managed encryption keys (CMEK) in GCP:

- Regional: Encryption keys that can only be used by resources in the same region.
- Global: Encryption keys that can be used by resources from multiple regions.

You can browse and use global or regional customer-managed encryption keys (CMEK) from all projects that are accessible to the service account. You can then use the key to create a CMEK enabled MCS machine catalog and update an existing CMEK enabled MCS machine catalog using `Set-ProvScheme` command. For information creating a CMEK enabled catalog using PowerShell, see Create a catalog with CMEK using custom properties.

For this feature, you need additional permissions for the following two service accounts:

- The service account of the current project with which the hosting connection is created.
- The Compute Engine Service Agent of the current project (that has the email: `service-PROJECT_NUMBER@compute-system.iam.gserviceaccount.com`). For more information, see Compute Engine Service Agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In Service accounts, you must assign the following roles in the project that has crypto keys that you want to use (for example, shared project):

- Cloud KMS Viewer
- Cloud KMS CryptoKey Encrypter/Decrypter

If you do not assign to the roles, then make sure that you have the following permissions:

- resourcemanager.projects.get
- cloudkms.keyRings.list
- cloudkms.keyRings.get
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

List the encryption keys

You can list the global and regional encryption keys within the same project and all other accessible projects using the PowerShell commands. To do this:

1. Open a PowerShell window from the Delivery Controller™ host or remote PowerShell.
2. Run the command `asnp citrix*` to load Citrix-specific PowerShell modules.
3. Run the following command to list the encryption keys. Example:

    - To list contents of `encryptionKeys` folder:

    ```
    Get-ChildItem XDHyp:\HostingUnits\my-
    hostingunit\encryptionKeys.folder
    ```

    - To get global encryption keys within the same project:

    ```
    Get-Item XDHyp:\HostingUnits\my-
    hostingunit\encryptionKeys.folder\myglobalkeyring.globalkeyring\mygl
    obalkey.cryptokey
    ```

    - To get regional encryption keys within the same project:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\regional-ring.keyring\shared-
key.cryptokey
```

- To get global encryption keys from another accessible project (for example: myanotherproject):

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject.project\shared-
global-ring.globalkeyring\shared-key.cryptokey
```

- To get regional encryption keys from another accessible project (for example: myanotherproject):

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject .project.project\
shared-uscentral.keyring\shared-uscentral-key.cryptokey
```

NOTE:

- The extension of the key ring inventory item for a global key ring is `.globalkeyring`.
- The id of global key rings has the word `global` in it.

Required GCP permissions

This section has the complete list of GCP permissions. Use the complete set of permissions as given in the section for the functionality to work correctly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

GCP is introducing changes to Cloud Build Services's default behavior and use of service accounts after April 29, 2024. For more information, see Cloud Build Service Account Change. Your existing Google projects with Cloud Build API enabled before April 29, 2024 are not affected by this change. However, if you want to have existing Cloud Build Service behavior after April 29, you can create or apply the organization policy to disable the constraint enforcement before you enable the API. If you set the new organization policy, you can still follow the existing permissions in this section and the items that are marked **Before Cloud Build Service Account Change**. If not, then follow the existing permissions and items that are marked **After Cloud Build Service Account Change**.

Creating a host connection

- Minimum permissions required for Citrix Cloud Service Account in Provisioning project:

  ```
  compute.instanceTemplates.list

  compute.instances.list

  compute.networks.list

  compute.projects.get

  compute.regions.list

  compute.subnetworks.list

  compute.zones.list

  resourcemanager.projects.get
  ```

  The following Google defined roles have the permissions as listed above:

  - Compute Admin
  - Cloud Datastore User

- Additional permissions required for Shared VPC for Citrix Cloud Service Account in Shared VPC project:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

The following Google defined roles have the permissions as listed above:

- Compute Network User

- In Service accounts, you must assign the following roles in the project that has crypto keys that you want to use (for example, shared project):
  - Cloud KMS Viewer
  - Cloud KMS CryptoKey Encrypter/Decrypter

  If you do not assign to the roles, then make sure that you have the following permissions:
  - resourcemanager.projects.get
  - cloudkms.keyRings.list
  - cloudkms.keyRings.get
  - cloudkms.cryptoKeys.get
  - cloudkms.cryptoKeys.list
  - cloudkms.cryptoKeyVersions.useToDecrypt
  - cloudkms.cryptoKeyVersions.useToEncrypt

Power management of VMs

Minimum permissions required for Citrix Cloud Service Account in Provisioning project in case of power managed only catalogs:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

The following Google defined roles have the permissions as listed above:

- Compute Admin
- Cloud Datastore User

Creating, updating, or deleting VMs

- Minimum permissions required for Citrix Cloud Service Account in Provisioning project:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

The following Google defined roles have the permissions as listed above:

- Compute Admin
- Storage Admin
- Cloud Build Editor
- Service Account User
- Cloud Datastore User

- Additional permissions required for Shared VPC for Citrix Cloud Service Account in Shared VPC project to create a hosting unit using VPC and subnetwork from Shared VPC project:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.zones.list

resourcemanager.projects.get
```

The following Google defined roles have the permissions as listed above:

- Compute Network User
- Cloud Datastore User

Minimum permissions required when downloading preparation instruction disk to MCS:

- (Before Cloud Build Service Account Change): Assign these permissions to Cloud Build Service Account in Provisioning project.
- (After Cloud Build Service Account Change): Assign these permissions to Cloud Compute Service Account in Provisioning project.

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

The following Google defined roles have the permissions as listed above:

- Cloud Build Service Account (After Cloud Build Service Account Change, it is Cloud Compute Service Account)
- Compute Instance Admin
- Service Account User

- Minimum permissions required for Cloud Compute Service Account in Provisioning project required by Google Cloud Build service when downloading preparation instruction disk to MCS:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

The following Google defined roles have the permissions as listed above:

- Compute Network User
- Storage Account User
- Cloud Datastore User

Additional permissions required for Shared VPC when downloading preparation instruction disk to MCS:

- (Before Cloud Build Service Account Change): Assign these permissions to Cloud Build Service Account in Provisioning project.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - (After Cloud Build Service Account Change): Assign these permissions to Cloud Compute Service Account in Provisioning project.

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

    The following Google defined roles have the permissions as listed above:

    - Compute Network User
    - Storage Account User
    - Cloud Datastore User

- Additional permissions required for Cloud Key Management Service (KMS) for Citrix Cloud Service Account in Provisioning project:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

    The following Google defined roles have the permissions as listed above:

    - Compute KMS Viewer

General permissions

Following are the permissions for Citrix Cloud Service Account in Provisioning project for all features supported in MCS. These permissions provide the best compatibility going forward:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use

cloudkms.cryptoKeyVersions.useToDecrypt

cloudkms.cryptoKeyVersions.useToEncrypt
```

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For Google Cloud Platform (GCP) specific information, see Create a Google Cloud Platform catalog.

More information

- Create and manage connections and resources
- Google Cloud virtualization environments.

Connection to HPE Moonshot

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to HPE Moonshot.

NOTE:

Before creating a connection to HPE Moonshot, you need to first finish setting up your HPE account. See HPE Moonshot virtualization environments.

Create a connection

You can create a connection to HPE Moonshot using:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Studio
- PowerShell commands

Create a connection using Studio

1. In the **Add Connection and Resources** page, select the **HPE Moonshot** as the connection type.
2. Enter the connection address of your Moonshot iLO Chassis Manager. You can use an IP address, host name, or FQDN for the address.
3. Enter your chassis administrative credentials and a friendly connection name.

Connection setup stops when either of the situations occurs:

- DaaS receives a public CA-signed certificate with errors: An error message appears. Follow the on-screen instructions to fix the issue. Otherwise, you can't proceed with connection creation.
- DaaS receives a private CA-signed certificate. A warning page appears. Compare the received thumbprint with the server's for the certificate validity. If it's valid, select **Trust certificate** and click **OK** to proceed with connection creation. DaaS will then trust the certificate and store the thumbprint for future validation.

Create a connection using PowerShell commands

When you create a connection using PowerShell command, provide the following information:

- IP: HPE Server IP Address
- Username: HPE username
- Password: HPE password

For example:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

NOTE:

The `sslthumbprint` parameter is required for only Private CA-signed certificates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Certificate and thumbprint validation

For creating a successful connection to **HPE Moonshot**, the certificate must not have errors and the thumbprint must have a correct value. Following are the use cases related to the certificate and thumbprint validation:

- Public CA-signed certificate has errors. The connection is not created successfully. See the error details and resolve the issue.
- Public CA-signed certificate without errors. The connection is created successfully, and the `SslThumbprints` value is **Null**.
- Private CA-signed certificate without errors and a `sslthumbprint` value. The connection is created successfully with a correct `SslThumbprints` value.
- Private CA-signed Certificate with an incorrect thumbprint value. The connection is not created successfully.
- Private CA-signed Certificate without errors. The connection is created successfully. The `SSlThumbprints` is **Null** when creating the connection. The `SSlThumbprints` value is updated to a value by the site service.

Manage connections

This section details how you can manage connections:

- Fix certificate issues using Studio
- Update thumbprint value using PowerShell command

Fix certificate issues

DaaS blocks an HPE Moonshot connection when certificate issues arise, preventing you from delivering and managing workloads on associated HPE Moonshot nodes. You'll see an error icon next to the connection in the **Host connections** list. See the following table for specific issues and solutions.

ISSUE	SOLUTION
A certificate error occurs to the public CA-signed certificate	Click the connection and select the **Troubleshoot** tab. View the error details and resolve the issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE	SOLUTION
The received certificate is private CA-signed or expired.	Edit the host connection to update the certificate thumbprint. Details steps: 1. Select the connection and click **Edit Connection**. 2. On the **Connection Properties** page, click **Edit settings**. 3. Enter the password to connect to the HPE Moonshot chassis, and then click **Save**. 4. On the **Warning** page that appears, compare the received thumbprint with the server's for certificate validity. 5. If they are the same, select **Trust certificate** and then click **OK**.

Update thumbprint values

After creating the connection, you can update the thumbprint value of a connection using the `Set-Item` PowerShell command. For example, run the following commands:

1. Get the connection details of a connection. For example:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. Update the thumbprint value. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. Check the updated thumbprint value. For example:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

NOTE:

The update fails if you provide an incorrect thumbprint value in the `Set-Item` command.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For HPE Moonshot specific information, see Create an HPE Moonshot machine catalog.

More information

- Create and manage connections and resources
- HPE Moonshot virtualization environments

Connection to Microsoft Azure Resource Manager

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Azure Resource Manager cloud environments.

NOTE:

Before creating a connection to Microsoft Azure, you must finish setting up your Azure account as a resource location. See Microsoft Azure Resource Manager virtualization environments.

Create service principals and connections

Before creating connections, you must set up service principals that connections use to access Azure resources. You can create a connection in two ways:

- Create a service principal and a connection together using Studio
- Create a connection using a previously created service principal

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This section shows you how to complete these tasks:

- Create a service principal and connection using Studio
- Create a service principal using PowerShell
- Get the application secret in Azure
- Create a connection using an existing service principal

Considerations

Before you start, be aware of these considerations:

- Citrix® recommends using service principals with a *Contributor* role. However, see the Minimum permissions section to get the list of minimum permissions.
- When creating the first connection, Azure prompts you to grant it the necessary permissions. For future connections you must still authenticate, but Azure remembers your previous consent and does not display the prompt again.
- After you authenticate with Azure for the first time, a Citrix owned multi-tenant application (ID: `08b70dc3-76c5-4611-ba7d-3312ba36cb2b`) is invited to your Microsoft Entra ID on behalf of the authenticated account.
- Accounts used for authentication must have permissions to assign roles in the subscription using Azure RBAC. Example, Owner, Role Based Access Control Administrator, or User Access Administrator of the subscription.
- The account used for authentication must be a member of the subscription's directory. There are two types of accounts to be aware of: 'Work or School' and 'personal Microsoft account.' See CTX219211 for details.
- While you can use an existing Microsoft account by adding it as a member of the subscription's directory, there can be complications if the user was previously granted guest access to one of the directory's resources. In this case, they might have a placeholder entry in the directory that does not grant them the necessary permissions, and an error is returned.

  Rectify this by removing the resources from the directory and adding them back explicitly. However, exercise this option carefully, because it has unintended effects on other resources that this account can access.
- There is a known issue where certain accounts are detected as directory guests when they are actually members. Configurations like this typically occur with older established directory accounts. Workaround: add an account to the directory, which takes the proper membership value.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Resource groups are simply containers for resources, and they can contain resources from regions other than their own region. This can potentially be confusing if you expect resources displayed in a resource group's region to be available.
- Ensure that your network and subnet are large enough to host the number of machines you require. This requires some foresight, but Microsoft helps you specify the right values, with guidance about the address space capacity.

Create a service principal and connection using Studio

IMPORTANT:

This feature is not yet available for Azure China subscriptions.

With Studio, you can create both a service principal and a connection in a single workflow. Service principals give connections access to Azure resources. When you authenticate to Azure to create a service principal, an application is registered in Azure. A secret key (called *client secret* or *application secret*) is created for the registered application. The registered application (a *connection* in this case) uses the client secret to authenticate to Microsoft Entra ID.

Before you start, make sure that you've met these prerequisites:

- You have a user account in your subscription's Microsoft Entra tenant.
- Accounts used for authentication must have permissions to assign roles in the subscription using Azure RBAC. Example, Owner, Role Based Access Control Administrator, or User Access Administrator of the subscription.
- You have global administrator, application administrator, or application developer permissions for authentication. The permissions can be revoked after you create a host connection. For more information about roles, see Microsoft Entra built-in roles.

Use the **Add Connection and Resources** wizard to create a service principal and a connection together:

1. On the **Connection** page, select **Create a new connection**, the **Microsoft Azure** connection type, and your Azure environment.
2. Select which tools to use to create the virtual machines and then select **Next**.
3. On the **Connection Details** page, select the **Application client secret** authentication mode, then create a service principal and set the connection name as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Enter your Azure subscription ID and a name for the connection. After you enter the subscription ID, the **Create new** button is enabled.

> **NOTE:**
>
> The connection name can contain 1–64 characters, and cannot contain only blank spaces or the characters `\/;:#.*?=<>|[]{}"'()'`.

a. Select **Create new** and then enter the Microsoft Entra account user name and password.

b. Select **Sign in**.

c. Select **Accept** to give Citrix DaaS™ the listed permissions. Azure creates a service principal that allows Citrix DaaS to manage Azure resources on behalf of the specified user.

> **NOTE:**
>
> Citrix DaaS requires the following permissions to create a new service principal:

- **Access Azure Service Management as you**
- **Read and write applications**
- **Sign you in and read your profile**
- **Maintain access to data you have given it access to**

d. After you select **Accept**, you're taken back to the **Connection Details** page.

> **NOTE:**
>
> After you successfully authenticate to Azure, the **Create new** and **Use existing** buttons disappear. The **Connection successful** text appears with a green check mark, indicating the successful connection to your Azure subscription.

e. To route API requests to Azure through Citrix Cloud™ Connectors, select the **Route traffic through Citrix Cloud Connectors** checkbox. When Cloud Connectors have no direct internet access, you can select **Use the proxy configured on Citrix Cloud Connectors** to ensure Azure connectivity works properly through Citrix Cloud Connectors.

Alternatively, you can enable this feature using PowerShell. For more information, see Create a secure environment for Azure-managed traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> This option is available only when there are active Citrix Cloud Connectors in your deployment. Currently, this feature is not supported for Connector Appliances.

f. Select **Next**.

> **NOTE:**
>
> You cannot proceed to the next page until you successfully authenticate to Azure and consent to giving the required permissions.

4. Configure the resources for the connection as follows:

   - On the **Region** page, select a region.
   - On the **Network** page, do the following:
     - Type a 1–64 character resource name to help identify the region and network combination. A resource name cannot contain only blank spaces or the characters `\/;:#.*?=<>|[]{}"'()'`.
     - Select a virtual network/resource group pair. (If you have more than one virtual network with the same name, pairing the network name with the resource group provides unique combinations.) If the region you selected on the previous page does not have any virtual networks, return to that page and select a region that has virtual networks.

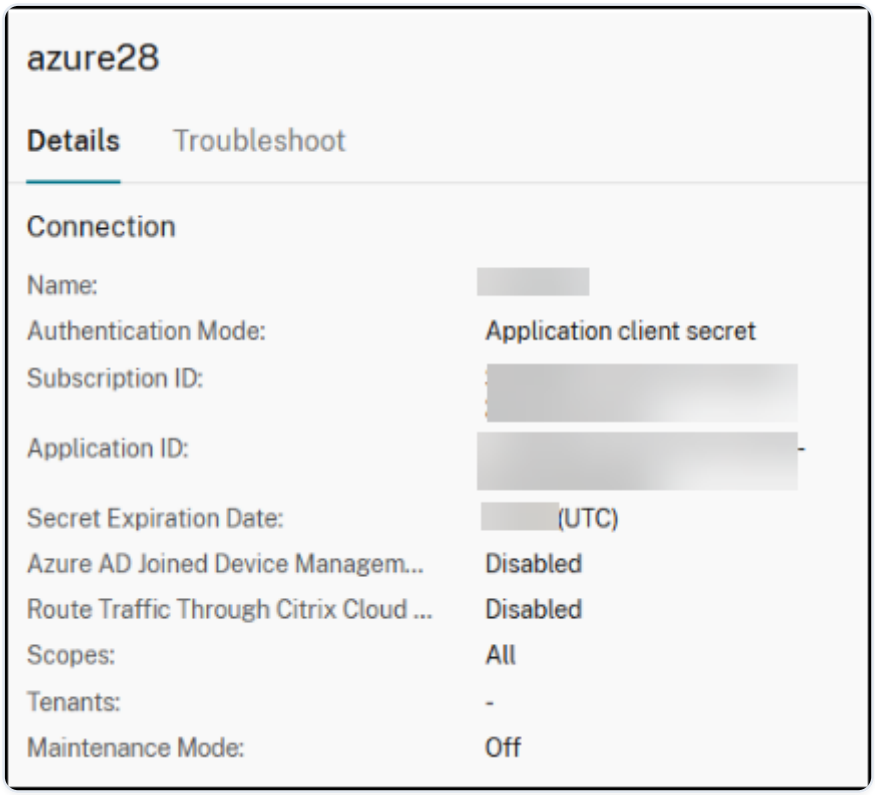
5. On the **Summary** page, view a summary of settings and select **Finish** to complete your setup.

VIEW THE APPLICATION ID

After you create a connection, you can view the application ID that the connection uses to access Azure resources.

In the **Connection and Resources** list, select the connection to view the details. The **Details** tab shows the Application ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create a service principal using PowerShell

To create a service principal using PowerShell, connect to your Azure Resource Manager subscription and use the PowerShell cmdlets provided in the following sections.

Make sure that you have these items ready:

- **SubscriptionId:** Azure Resource Manager `SubscriptionID` for the subscription where you want to provision VDAs.
- **ActiveDirectoryID**: Tenant ID of the application that you registered with Microsoft Entra ID.
- **ApplicationName:** Name for the application to be created in Microsoft Entra ID.

Detailed steps are as follows:

1. Connect to your Azure Resource Manager subscription.

   ```
   Connect-AzAccount
   ```

2. Select the Azure Resource Manager subscription where you want to create the service principal.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

3. Create the application in your AD tenant.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Create a service principal.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

5. Assign a role to the service principal.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

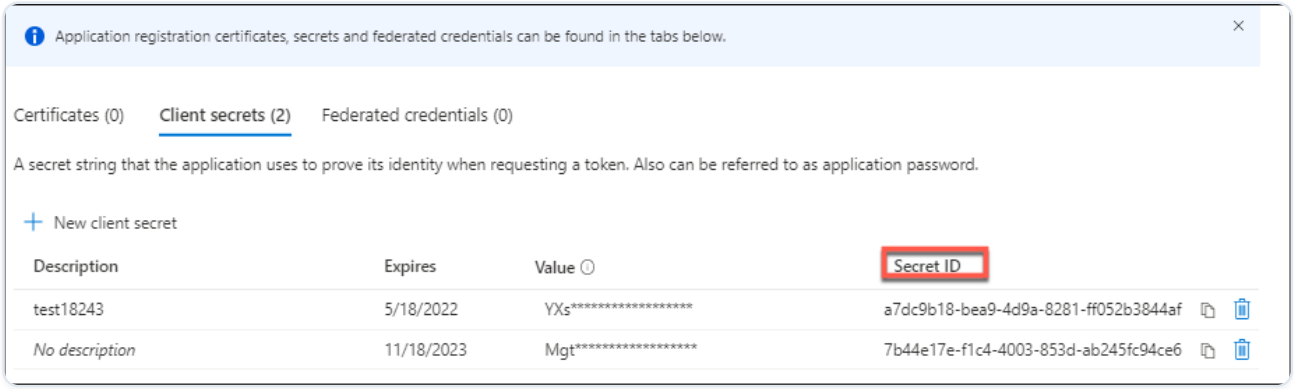
6. From the output window of the PowerShell console, note the ApplicationId. You provide that ID when creating the host connection.

Get the application secret in Azure

To create a connection using an existing service principal, you must first get the application ID and secret of the service principal in the Azure portal.

Detailed steps are as follows:

1. Get the **Application ID** from Studio or using PowerShell.
2. Sign in to the Azure portal.
3. In Azure, select **Microsoft Entra ID**.
4. From **App registrations** in Microsoft Entra ID, select your application.
5. Go to **Certificates & secrets**.
6. Click **Client secrets**.



Create a connection using an existing service principal

If you already have a service principal, you can use it to create a connection using Studio.

Make sure that you have these items ready:

- SubscriptionId
- ActiveDirectoryID (tenant ID)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Application ID
- Application secret

  For more information, see Get the application secret.
- Secret expiration date

Detailed steps are as follows:

In the **Add Connection and Resources** wizard:

1. On the **Connection** page, select **Create a new connection**, the **Microsoft Azure** connection type, and your Azure environment.
2. Select which tools to use to create the virtual machines and then select **Next**.
3. On the **Connection Details** page, select the **Application client secret** authentication mode, then enter your Azure subscription ID and a name for the connection.

   NOTE:

   The connection name can contain 1–64 characters, and cannot contain only blank spaces or the characters `\/;:#.*?=<>|[]{}"'()'`.
4. Select **Use existing**. In the **Existing Service Principal Details** window, enter the following settings for the existing service principal. After you enter the details, the **Save** button is enabled. Select **Save**. You cannot progress beyond this page until you provide valid details.

   - **Subscription ID**. Enter your Azure subscription ID. To obtain your subscription ID, sign in to the Azure portal and navigate to **Subscriptions > Overview**.
   - **Active Directory ID** (tenant ID). Enter the Directory (tenant) ID of the application that you registered with Microsoft Entra ID.
   - **Application ID**. Enter the Application (client) ID of the application that you registered with Microsoft Entra ID.
   - **Application secret**. Enter a secret key (client secret). The registered application uses the key to authenticate to Microsoft Entra ID. We recommend that you change keys regularly for security purposes. Be sure to save the key because you cannot retrieve the key later.
   - **Secret expiration date**. Enter the date after which the application secret expires. You receive an alert on the console starting 14 days before the secret key expires. However, if the secret key expires, you receive errors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> For security purposes, the expiration period cannot be more than two years from now.

- **Authentication URL**. This field is automatically populated and isn't editable.
- **Management URL**. This field is automatically populated and isn't editable.
- **Storage suffix**. This field is automatically populated and isn't editable.
- **Azure blob storage endpoint to upload or download disks or snapshots**. This field is automatically populated and isn't editable.
- **Key Vault Service**. This field is automatically populated and isn't editable.
- **Service bus suffix**. This field is automatically populated and isn't editable.

  Access to the following endpoints is required for creating an MCS catalog in Azure. Access to these endpoints optimizes connectivity between your network and the Azure portal and its services.

  - Authentication URL: `https://login.microsoftonline.com`
  - Management URL: `https://management.azure.com`. This is a request URL for Azure Resource Manager provider APIs. The endpoint for management depends on the environment. For example, for Azure Global, it is `https://management.azure.com`, and for Azure US Government, it is `https://management.usgovcloudapi.net`.
  - Storage suffix: `https://*.core.windows.net`. This (*) is a wildcard character for storage suffix. For example, `https://demo.table.core.windows.net`.
  - Azure blob storage endpoint to upload or download disks or snapshots: `https://*.storage.azure.net`. This (*) is a wildcard character for blob storage import and export operations. For example, `https://md-impexp-xxxxx.z[00-50].blob.storage.azure.net`.
  - Key vault service: `https://*.vault.azure.net`. This (*) is a wildcard character for the key vault name. For example, `https://<your-key-vault-name>.vault.azure.net`.
  - Service bus suffix: `https://*.servicebus.windows.net`. This (*) is a wildcard character for namespaces created in the global Azure cloud. For example, `https://{serviceNamespace}.servicebus.windows.net/{path}`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. After selecting **Save**, you're taken back to the **Connection Details** page. Select **Next** to proceed to the next page.
6. Configure the resources for the connection as follows:
    - On the **Region** page, select a region.
    - On the **Network** page, do the following:
        - Type a 1–64 character resource name to help identify the region and network combination. A resource name cannot contain only blank spaces or the characters `\/;:#.*?=<>|[]{}"'()'`.
        - Select a virtual network/resource group pair. (If you have more than one virtual network with the same name, pairing the network name with the resource group provides unique combinations.) If the region you selected on the previous page does not have any virtual networks, return to that page and select a region that has virtual networks.
7. On the **Summary** page, view a summary of settings and select **Finish** to complete your setup.

Manage service principals and connections

This section details how you can manage service principals and connections:

- Configure Azure throttling settings
- Manage service principal of an existing hosting connection
- Enable image sharing in Azure
- Add shared tenants to a connection using Studio
- Implement image sharing using PowerShell
- Create a secure environment for Azure-managed traffic
- Manage the application secret and secret expiration date

Configure Azure throttling settings

Azure Resource Manager throttles requests for subscriptions and tenants, routing traffic based on defined limits, tailored to the specific needs of the provider. See Throttling Resource Manager requests on the Microsoft site for more information. Limits exist for subscriptions and tenants, where managing many machines can become problematic. For example, a subscription containing many machines might experience performance problems related to power operations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP:

For more information, see Improving Azure performance with Machine Creation Services.

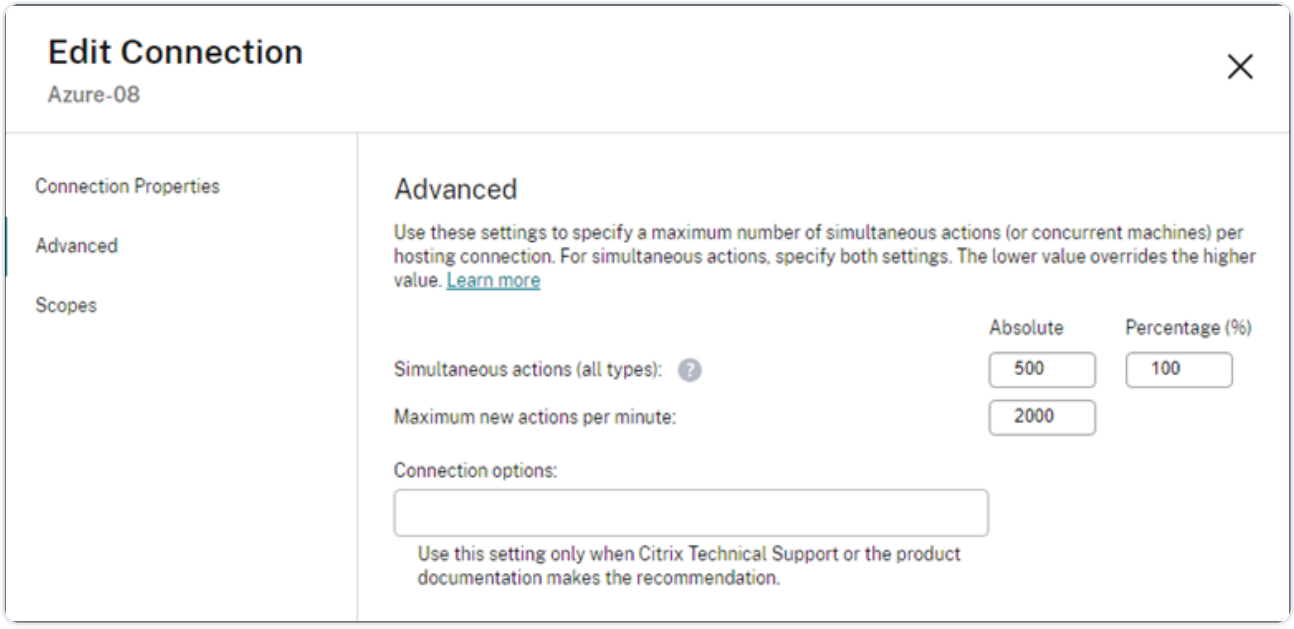
To help mitigate these issues, Citrix DaaS allows you to remove MCS internal throttling to use more of the available request quota from Azure.

We recommend the following optimal settings when powering VMs on or off in large subscriptions, for example, those containing 1,000 VMs:

- Absolute simultaneous operations: 500
- Maximum new operations per minute: 2000
- Max concurrency of operations: 500

Use Studio to configure Azure operations for a given host connection:

1. From Studio, select **Hosting** in the left pane.
2. Select an Azure-related connection to edit it.
3. In the **Edit Connection** wizard, select **Advanced**.
4. On the **Advanced** page, use the configuration options to specify the number of simultaneous actions and maximum new actions per minute, and any additional connection options.



MCS supports 500 maximum concurrent operations by default. Alternatively, you can use the Remote PowerShell SDK to set the maximum number of concurrent operations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use the **PowerShell** property, `MaximumConcurrentProvisioningOperations`, to specify the maximum number of concurrent Azure provisioning operations. When using this property, consider:

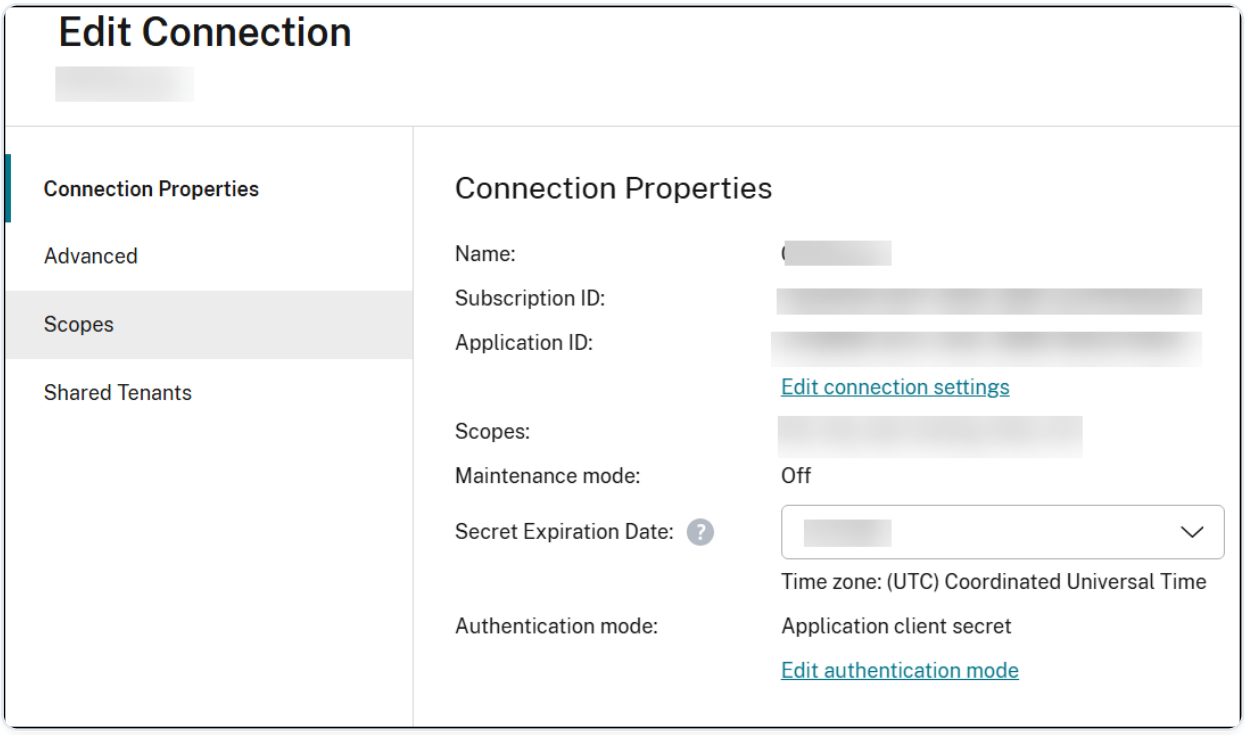
- Default value of `MaximumConcurrentProvisioningOperations` is 500.
- Configure the `MaximumConcurrentProvisioningOperations` parameter using the PowerShell command `Set-item`.

Manage the service principal of an existing hosting connection

After creating a hosting connection using a service principal, you can choose to edit the hosting connection to have:

- New service principal
- Use another existing service principal

1. From Studio, select **Hosting** from the left pane.
2. Select the connection and then select **Edit Connection** in the action bar.
3. Select **Connection Properties** from the left pane.
4. On the **Connection Properties** page that appears, click **Edit conenction settings**. You can now choose to create a new service principal or use another existing service principal.



   - Click **Create service principal** to create a new service principal. Follow the prompt to log in to your Microsoft Entra user account. Citrix uses the multi-tenant application ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`08b70dc3-76c5-4611-ba7d-3312ba36cb2b` to create a new service principal for the existing host connection and grant proper permissions.

- Click **Use existing** to use another existing service principal for that hosting connection.

Enable image sharing in Azure

When creating or updating machine catalogs, you can select shared images from different Azure tenants and subscriptions (shared through the Azure Compute Gallery). To enable image sharing within or across tenants, you must make the necessary settings in Azure:

- Share images within a tenant (across subscriptions)
- Share images across tenants

SHARE IMAGES WITHIN A TENANT (ACROSS SUBSCRIPTIONS)

To select an image in Azure Compute Gallery that belongs to a different subscription, the image must be shared with the service principal (SPN) of that subscription.

For example, if there is a service principal (SPN 1), which is configured in Studio as:

Service principal: SPN 1

Subscription: subscription 1

Tenant: tenant 1

The image is in a different subscription, which is configured in Studio as:

Subscription: subscription 2

Tenant: tenant 1

If you want to share the image in subscription 2 with subscription 1 (SPN 1), go to subscription 2, and share the resource group with SPN1.

The image must be shared with another SPN using Azure role-based access control (RBAC). Azure RBAC is the authorization system used to manage access to Azure resources. For more information on Azure RBAC, see the Microsoft document What is Azure role-based access control (Azure RBAC). To grant access, you assign roles to service principals at resource group scope with the Contributor role. To assign Azure roles, you must have `Microsoft.Authorization/roleAssignments/write` permission, such as User Access Administrator or Owner. For more information on sharing images with another SPN, see the Microsoft document Assign Azure roles using the Azure portal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SHARE IMAGES ACROSS TENANTS

To share images across tenants with Azure Compute Gallery, create or update the application registration and use this application to create hosting connection.

For example, if there are two tenants (Tenant 1 and Tenant 2) and you want to share your image gallery with Tenant 1, then:

1. Create an application registration for Tenant 1. For more information, see Create the app registration.
2. Give Tenant 2 access to the application by requesting a sign-in using a browser. Replace `Tenant2 ID` with the tenant ID of Tenant 1. Replace `Application (client) ID` with the application ID of the application registration that you created. When done making the replacements, paste the URL into a browser and follow the sign-in prompts to sign into Tenant 2. For example:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   For more information, see Give Tenant 2 access.
3. Give the application access to the Tenant 2 resource group. Sign in as Tenant 2 and give the application registration access to the resource group that has the gallery image. For more information, see Authenticate requests across tenants.

Add shared tenants to a connection using Studio

When creating or updating machine catalogs in Studio, you can select shared images from different Azure tenants and subscriptions (shared through the Azure Compute Gallery). The feature requires that you provide shared tenant and subscription information for associated host connections.

NOTE:

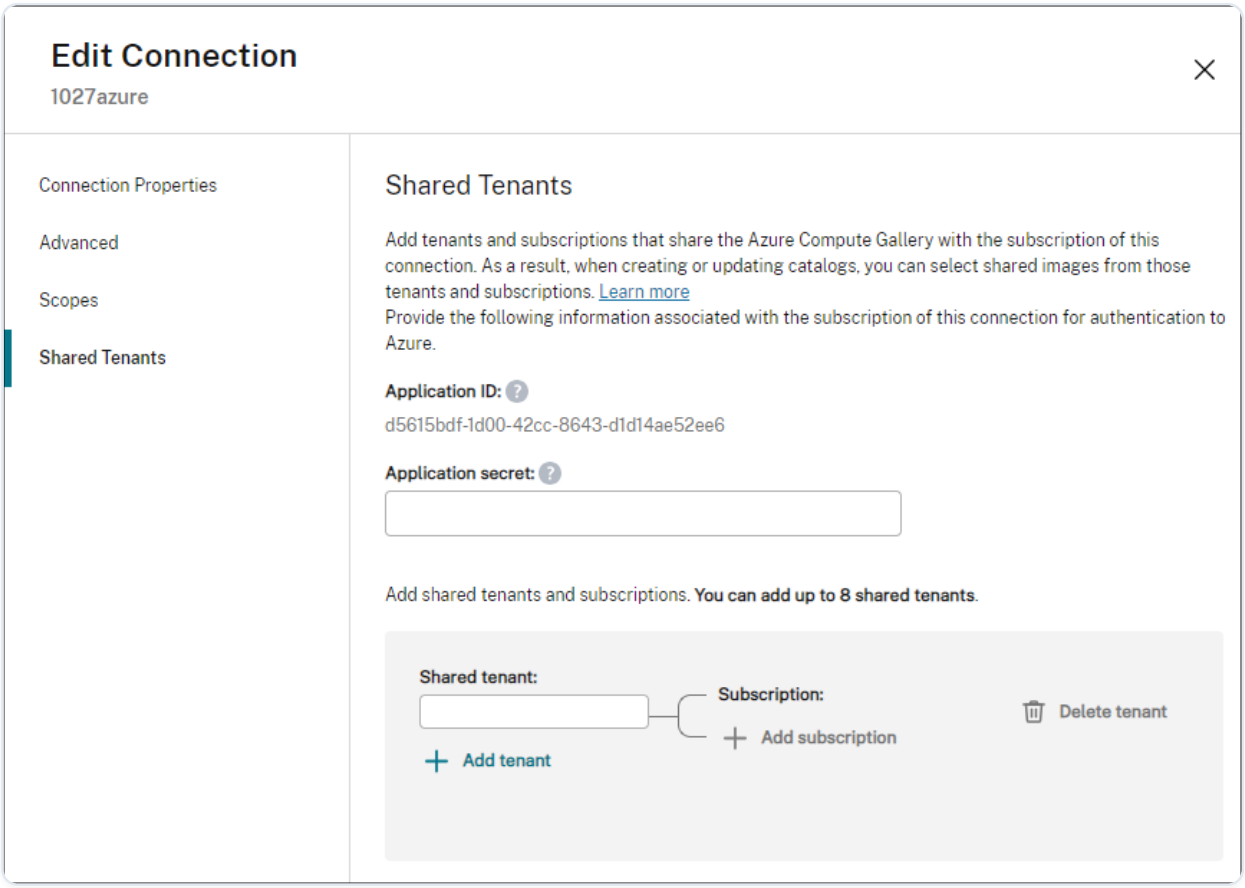
Make sure you've configured the necessary settings in Azure to enable image sharing across tenants. For more information, see Share images across tenants.

Complete the following steps for a connection:

1. From Studio, select **Hosting** in the left pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the connection and then select **Edit Connection** in the action bar.



3. In **Shared Tenants**, do the following:

   a. Provide the application ID and application secret associated with the subscription of the connection. DaaS uses this information to authenticate to Microsoft Entra ID.

   b. Add tenants and subscriptions that share the Azure Compute Gallery with the subscription of the connection. You can add up to eight shared tenants and eight subscriptions for each tenant.

4. When you are finished, select **Apply** to apply the changes you made and keep the window open, or select **OK** to apply the changes and close the window.

Implement image sharing using PowerShell

This section guides you through the processes of sharing images using PowerShell:

- Select an image from a different subscription
- Update hosting connection custom properties with shared tenant IDs
- Select an image from a different tenant

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SELECT AN IMAGE FROM A DIFFERENT SUBSCRIPTION

You can select an image in Azure Compute Gallery that belongs to a different shared subscription in the same Azure tenant to create and update MCS catalogs using PowerShell commands.

1. In the hosting unit root folder, Citrix creates a new shared subscription folder called `sharedsubscription`.
2. List all shared subscriptions in a tenant.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. Select one shared subscription, and then list all shared resource groups of that shared subscription.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. Select a resource group, and then list all galleries of that resource group.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. Select a gallery, and then list all image definitions of that gallery.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. Select one image definition, and then list all image versions of that image definition.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. Create and update an MCS catalog using the following elements:
    - Resource group

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Gallery
- Gallery image definition
- Gallery image version

UPDATE HOSTING CONNECTION CUSTOM PROPERTIES WITH SHARED TENANT IDS

Use `Set-Item` to update the hosting connection custom properties with shared tenant IDs and subscription IDs. Add a property `SharedTenants` in `CustomProperties`. The format of `SharedTenants` is:

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

For example:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />

</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-SecurePassword

$psd
```

NOTE:

You can add more than one tenant. Each tenant can have more than one subscription.

SELECT AN IMAGE FROM A DIFFERENT TENANT

You can select an image in the Azure Compute Gallery that belongs to a different Azure tenant to create and update MCS catalogs using PowerShell commands.

1. In the hosting unit root folder, Citrix creates a new shared subscription folder called `sharedsubscription`.
2. List all shared subscriptions.

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. Select one shared subscription, and then list all shared resource groups of that shared subscription.

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription
   ```

4. Select a resource group, and then list all galleries of that resource group.

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription\
   xyz.resourcegroup
   ```

5. Select a gallery, and then list all image definitions of that gallery.

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
   group\efg.gallery
   ```

6. Select one image definition, and then list all image versions of that image definition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. Create and update an MCS catalog using the following elements:
   - Resource group
   - Gallery
   - Gallery image definition
   - Gallery image version

Create a secure environment for Azure-managed traffic

MCS enables network traffic (API calls from Citrix Cloud to Azure hypervisor) to be routed through Cloud Connectors in your environment. This implementation helps you lock down your Azure subscription to allow network traffic from specific IP addresses. To do this, add `ProxyHypervisorTrafficThroughConnector` in `CustomProperties`. After you set the custom properties, you can configure Azure policies to have private disk access to Azure managed disks.

If you configure the Azure policy to create Disk Accesses automatically for each new disk to use private endpoints, you cannot upload or download more than five disks or snapshots at the same time with the same disk access object as enforced by Azure. This limit is for each machine catalog if you configure Azure policy at resource group level, and for all machine catalogs if you configure Azure policy at subscription level. If you do not configure the Azure policy to create Disk Accesses automatically for each new disk to use private endpoints, the limit of five concurrent operations is not enforced.

NOTE:

Currently, this feature is not supported for Connector Appliance. For Azure limitations related to this feature, see Restrict import/export access for managed disks using Azure Private Link.

ENABLE THE PROXY

To enable the proxy, set the custom properties as follows on the host connection:

1. Open a PowerShell window using the Remote PowerShell SDK. For more information, see `<https://docs.citrix.com/en-us/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/>`.
2. Run the following commands:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Add-PSSnapin citrix*.

cd XDHyp:\Connections\

dir
```

3. Copy the `CustomProperties` from the connection to a notepad and append property setting `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector" Value="True" />` to the `CustomProperties` to enable the proxy. For example:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="SubscriptionId"
Value="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />

<Property xsi:type="StringProperty" Name="ManagementEndpoint"
Value="https://management.azure.com/" />

<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
Value="https://login.microsoftonline.com/" />

<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />

<Property xsi:type="StringProperty" Name="TenantId"
Value="5cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx" />

<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />

</CustomProperties>
```

4. In the PowerShell window, assign a variable to the modified custom properties. For example:

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">

<Property xsi:type="StringProperty" Name="SubscriptionId"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Value="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />

<Property xsi:type="StringProperty" Name="ManagementEndpoint"
Value="https://management.azure.com/" />

<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
Value="https://login.microsoftonline.com/" />

<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />

<Property xsi:type="StringProperty" Name="TenantId"
Value="5cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx" />

<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />

</CustomProperties>'
```

5. Run `$cred = Get-Credential`. If prompted, provide the connection credentials. The credentials are Azure Application ID and secret.
6. Run `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password`.

IMPORTANT:

If you get a message stating `SubscriptionId` is missing, then replace all double quotes (“) with backtick followed by double quotes (`”) in the custom property. For example:

```
<CustomProperties xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`" xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`"
Value=`"5cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx`" />

<Property xsi:type=`"StringProperty`"
Name=`"ProxyHypervisorTrafficThroughConnector`" Value=`"True`" />

</CustomProperties>
```

7. Run `dir` to verify the updated `CustomProperties` settings.

Option to use system proxy on Citrix Cloud Connectors for redirected Azure API traffic

To route all external traffic through a non-transparent proxy, configure the host connection with the custom property `UseSystemProxyForHypervisorTrafficOnConnectors`. This redirects Azure API internet traffic on Citrix Cloud Connectors through the system proxy.

Do the same steps as outlined in Enable the proxy to configure the host connection with the custom property. However, make sure to append property setting `<Property xsi:type="StringProperty" Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />` to the `CustomProperties` to enable the proxy.

```
<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />
```

Example:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="SubscriptionId"
Value="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />

<Property xsi:type="StringProperty" Name="ManagementEndpoint"
Value="https://management.azure.com/" />

<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
Value="https://login.microsoftonline.com/" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />

<Property xsi:type="StringProperty" Name="TenantId"
Value="5cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx" />

<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />

<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />

</CustomProperties>
```

NOTE:

After you set this property, the proxy configured in the `netsh winhttp` settings on the Citrix Cloud Connectors is used for outbound traffic to the cloud service provider.

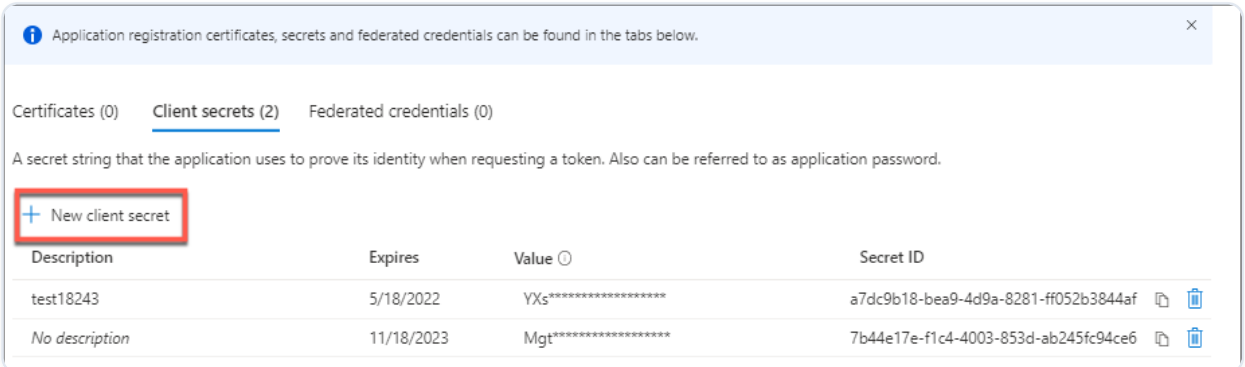
Manage the application secret and secret expiration date

Be sure to change the application secret for a connection before the secret expires. You receive an alert on Studio before the secret key expires.

CREATE AN APPLICATION SECRET IN AZURE

You can create an application secret for a connection through the Azure portal.

1. Select **Microsoft Entra ID**.
2. From **App registrations** in Microsoft Entra ID, select your application.
3. Go to **Certificates & secrets**.
4. Click **Client secrets > New client secret**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Provide a description of the secret and specify a duration. When you're done, select **Add**.

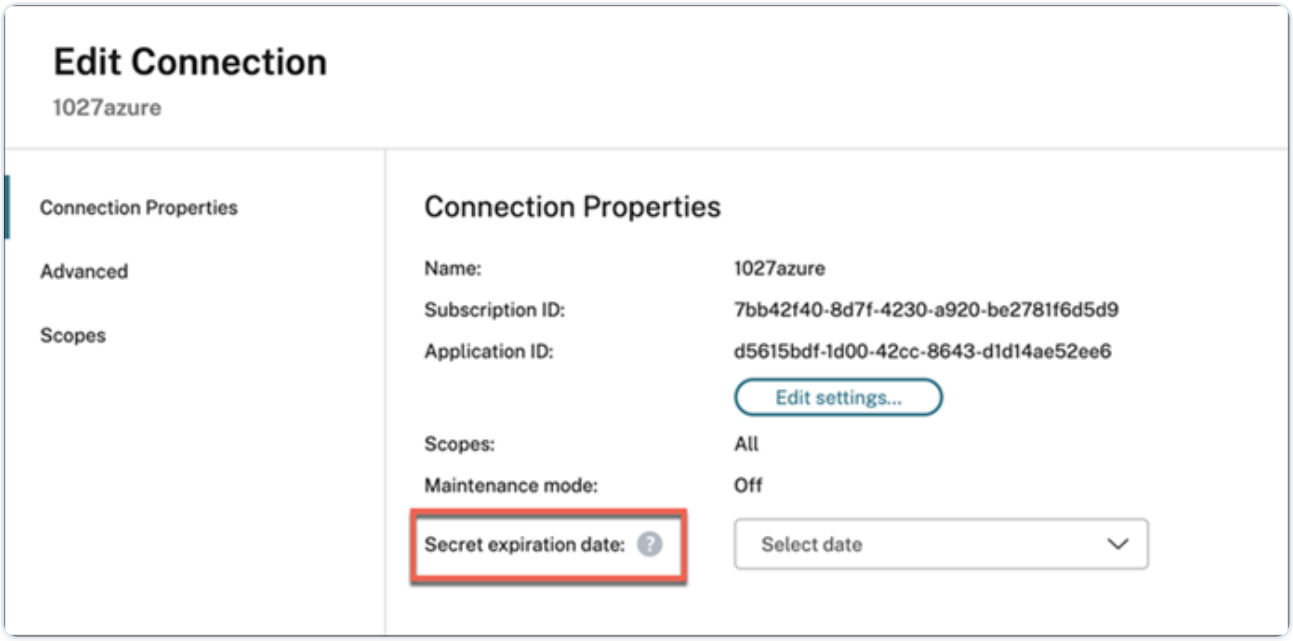
> **NOTE:**
>
> Be sure to save the client secret because you cannot retrieve it later.

6. Copy the client secret value and the expiration date.
7. In Studio, edit the corresponding connection and replace the content in the **Application secret** and **Secret expiration date** field with the values you copied.

CHANGE THE SECRET EXPIRATION DATE

You can use Studio to add or modify the expiration date for the application secret in use.

1. In the **Add Connection and Resources** wizard, right-click a connection, and click **Edit Connection**.
2. On the **Connection Properties** page, click **Secret expiration date** to add or modify the expiration date for the application secret in use.



Create a host connection using Azure Managed Identity

You can create a host connection to Microsoft Azure Resource Manager using Azure Managed Identity. The Azure managed identities offer a secure and scalable way to access Azure services without the need to manage credentials. This approach eliminates the risks associated with storing, rotating, and managing secrets.

The **Authentication Mode** has three options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- AppClientSecret
- SystemAssignedManagedIdentity
- UserAssignedManagedIdentity

Before you begin

Following are the steps you must do before creating the host connection using the Azure Managed Identity:

1. Install a Citrix Cloud Connector™ in an Azure VM.
2. Enable Azure Managed Identity on that Cloud Connector VM.
    - For the user assigned managed identity:
        a. On the Azure portal, create a user assigned managed identity. For information, see Create and assign a User Assigned Managed Identity.
        b. Assign Azure roles to the managed identity. See Required Azure permissions.
        c. Create an Azure VM as a Cloud Connector and add the user assigned identity to it.
    - For the system assigned managed identity:
        a. Open the Azure portal and go to your VM.
        b. Select the Identity blade in the VM's settings.
        c. Under the **System assigned** tab, set the status to **On**.
        d. Click **Save**.
        e. Grant Required Azure permissions.

        NOTE:

        If you enable the system assigned managed identity on a Cloud Connector VM and use it to create a host connection, you can still create host connections with the system assigned managed identity even after disabling it on the Cloud Connector VM. The creation of host connections can succeed even 24 hours after the identity has been disabled. This happens because managed identity tokens are cached by the underlying Azure infrastructure. For more information, see Are managed identities tokens cached?.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create the host connection with Azure Managed Identity using Studio

In the **Add Connection and Resources** wizard:

1. On the **Connection** page:
    a. Select **Create a new connection**, the Microsoft Azure connection type, and your Azure environment.
    b. Select which tools to use to create the virtual machines and then select Next.
2. On the **Connection Details** page, select the **Authentication mode**.
    - For the **User assigned managed identity**, enter the following settings. After you enter the details, select **Next** to proceed to the following pages. You cannot progress beyond this page until you provide valid details.
        - **Subscription ID**: Enter your Azure subscription ID. To obtain your subscription ID, sign in to the Azure portal and navigate to **Subscriptions > Overview**.
        - **Active Directory ID** (tenant ID): Enter the Directory (tenant) ID of the application that you registered with Microsoft Entra ID.
        - **Client ID**: Enter the Client ID of the Managed Identity that you created in the Azure portal.
        - **Authentication URL**: This field is automatically populated and isn't editable.
        - **Management URL**: This field is automatically populated and isn't editable.
        - **Storage suffix**: This field is automatically populated and isn't editable.
    - For the **System assigned managed identity**, enter the following settings. After you enter the details, select **Next** to proceed to the following pages. You cannot progress beyond this page until you provide valid details.
        - **Subscription ID**: Enter your Azure subscription ID. To obtain your subscription ID, sign in to the Azure portal and navigate to **Subscriptions > Overview**.
        - **Active Directory ID** (tenant ID): Enter the Directory (tenant) ID of the application that you registered with Microsoft Entra ID.
        - **Authentication URL**: This field is automatically populated and isn't editable.
        - **Management URL**: This field is automatically populated and isn't editable.
        - **Storage suffix**: This field is automatically populated and isn't editable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create the host connection with Azure Managed Identity using PowerShell

You can create this host connection using a new CustomProperty `AuthenticationMode`. The `AuthenticationMode` has three options: `AppClientSecret`, `SystemAssignedManagedIdentity`, and `UserAssignedManagedIdentity`. The following is the description of the authentication mode options:

- `AppClientSecret`: This is the default value. This needs an Application ID and secret.
- `UserAssignedManagedIdentity`: This needs a client ID to be provided through a UserName.
- `SystemAssignedManagedIdentity`: This doesn't need any input. Even if you provide a client id, it is ignored.

NOTE:

While using PowerShell, the parameter `ProxyHypervisorTrafficThroughConnector` must be true to use managed identity.

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create host connections. For example:
    - For the user assigned managed identity:

```
$UserName = "should be the Client ID of the user-assigned managed
identity"

$Password = "It can be any string.Not used"



$CustomProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">' `

+ '<Property xsi:type="StringProperty" Name="SubscriptionId"
Value="' + $SubscriptionId + '" />'`

+ '<Property xsi:type="StringProperty" Name="ManagementEndpoint"
Value="https://management.azure.com/" />'`
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
+ '<Property xsi:type="StringProperty"
Name="AuthenticationAuthority" Value="https://
login.microsoftonline.com/" />'`

+ '<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />'`

+ '<Property xsi:type="StringProperty" Name="TenantId" Value="' +
$TenantId + '" />'`

+ '<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />'`

+ '<Property xsi:type="StringProperty" Name="AuthenticationMode"
Value="UserAssignedManagedIdentity" />'`

+ '</CustomProperties>'



New-Item -ConnectionType "Custom" `

-CustomProperties $CustomProperties `

-HypervisorAddress @($HypervisorAddress) `

-Path @("XDHyp:\Connections\$($ConnectionName)") `

-Metadata $Metadata `

-Persist `

-PluginId "AzureRmFactory" `

-Scope @() `

-Password $Password `

-UserName $UserName `

-ZoneUid $zoneUid
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For the system assigned managed identity:

```
$UserName = "It can be any string. Not used"

$Password = "It can be any string. Not used"

$CustomProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">' `

+ '<Property xsi:type="StringProperty" Name="SubscriptionId"
Value="' + $SubscriptionId + '" />'`

+ '<Property xsi:type="StringProperty" Name="ManagementEndpoint"
Value="https://management.azure.com/" />'`

+ '<Property xsi:type="StringProperty"
Name="AuthenticationAuthority" Value="https://
login.microsoftonline.com/" />'`

+ '<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />'`

+ '<Property xsi:type="StringProperty" Name="TenantId" Value="' +
$TenantId + '" />'`

+ '<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />'`

+ '<Property xsi:type="StringProperty" Name="AuthenticationMode"
Value="SystemAssignedManagedIdentity" />'`

+ '</CustomProperties>'



New-Item -ConnectionType "Custom" `

-CustomProperties $CustomProperties `

-HypervisorAddress @($HypervisorAddress) `

-Path @("XDHyp:\Connections\$($ConnectionName)") `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-Metadata $Metadata `
-Persist `
-PluginId "AzureRmFactory" `
-Scope @() `
-Password $Password `
-UserName $UserName `
-ZoneUid $zoneUid
```

Manage Azure Managed Identity of an existing hosting connection

Use Studio

After creating a hosting connection, you can choose to update the existing hosting connection to have:

- System assigned managed identity
- User assigned managed identity
- A new user assigned managed identity

1. From Studio, select **Hosting** from the left pane.
2. Select the connection and then select **Edit Connection** in the action bar.
3. On the **Connection Properties** page that appears, click **Edit authentication mode**. You can now choose to update the authentication mode.
    - Click **User assigned managed identity** to use User assigned managed identity for that hosting connection. Follow the Client ID to be filled.
    - Click **System assigned managed identity** to use System assigned managed identity for that hosting connection.

Use PowerShell

You can also update an existing host connection using PowerShell to use a system assigned identity or user assigned managed identity. For example, run the following PowerShell commands:

1. Open a PowerShell window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run the following commands:

```
$connName = "ConnectionName"

$conn = get-item XDHyp:\Connections\$connName

$conn.CustomProperties
```

4. Change `ProxyHypervisorTrafficThroughConnector` to `True` and add the custom property for `AuthenticationMode` set to `SystemAssignedManagedIdentity` or `UserAssignedManagedIdentity`. For example:

```
$customProps = '<CustomProperties xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation"><Property xsi:type="StringProperty"
Name="SubscriptionId" Value="subscriptionId" /><Property
xsi:type="StringProperty" Name="ManagementEndpoint" Value="https://
management.azure.com/" /><Property xsi:type="StringProperty"
Name="AuthenticationAuthority" Value="https://
login.microsoftonline.com/" /><Property xsi:type="StringProperty"
Name="StorageSuffix" Value="core.windows.net" /><Property
xsi:type="StringProperty" Name="TenantId" Value="tenantId" /><Property
xsi:type="StringProperty" Name="AzureAdDeviceManagement"
Value="false" /><Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="true" /><Property
xsi:type="StringProperty" Name="AuthenticationMode"
Value="SystemAssignedManagedIdentity" /></CustomProperties>'
```

5. Run `$cred = Get-Credential`. Enter anything here.
6. Run `Set-Item -PSPath XDHyp:\Connections\$connName -CustomProperties $CustomProperties -username $cred.username -Securepassword $cred.password`.

Azure Extended Zones

Azure Extended Zones are small-footprint extensions of existing Azure regions, enabling organizations to run workloads closer to their users for improved performance and compliance. MCS on Azure now supports provisioning and power management for VMs in Extended Zones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To learn more about Azure Extended Zones, see the Microsoft documentation: Azure Extended Zones documentation.

Use cases

This feature is applicable for persistent and non-persistent catalogs:

- Power-managed only VMs: You can import your existing extended zone VMs into a power-managed-only catalog and power-manage them with Citrix MCS.
- MCS Provisioned VMs: You can provision new VMs into an Extended Zone and manage them with MCS. This feature also includes support for image management workflows.

Limitations

There are currently several limitations for using Azure Extended Zones. Many of these limitations are due to current Azure constraints:

- Dedicated hosts are not supported.
- Capacity reservations are not supported.
- Proximity placement groups are not supported.
- Spot VMs are not supported.
- Availability Zones are not supported in Extended Zones.
- Only **StandardSSD_LRS** and **Premium_LRS** storage types are supported.
- You cannot currently use the **UseSharedImageGallery** feature to save a mastered image into an Azure Compute Gallery (or Shared Image Gallery) in an Extended Zone. As a byproduct, Ephemeral OS disks are also not supported.
- If you are using an Azure Compute Gallery image version as your master image, ensure that replication has fully completed in the Extended Zone before attempting to use it. Attempting to use the image version before replication completes might result in deployment failure.

Prerequisites

Before using Extended Zones, ensure you have completed the following prerequisite steps:

1. Register with Azure:
    a. Extended Zones are not enabled by default.
    b. Register the `Microsoft.EdgeZones` resource provider in your Azure subscription: Register your subscription for resource provider Microsoft.EdgeZones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Register each required Extended Zone separately (ex: LosAngeles, Perth): Register for an Azure Extended Zone.

2. Prepare Citrix resources:

   a. Create a virtual network in your Extended Zone.

   b. Create master images and snapshots as needed.

Required permissions

To create a catalog in an Extended Zone, your service principal must have the following permission: `Microsoft.EdgeZones/extendedZones/read`.

For more on minimum required permissions, see Minimum permissions.

Configuration steps

1. Create a Hosting Unit in an Extended Zone

   Extended Zones, which use the `.extendedzone` type, are listed alongside regions in the Citrix MCS inventory. To provision into an extended zone, you must create a new hosting unit tied to that extended zone.

   Example: To create a hosting Unit in Los Angeles Extended Zone

```
$RootPath = "XDHyp:\Connections\MyConnectionName\Los
Angeles.extendedzone"



$NetworkPath = "XDHyp:\Connections\MyConnectionName\Los
Angeles.extendedzone\virtualprivatecloud.folder\MyResourceGroup.resourc
egroup\MyExtendedZoneNetwork.virtualprivatecloud\MyExtendedZoneSubnet.n
etwork"



$HostingUnitPath = "XDHyp:\HostingUnits\MyHostingUnitName"



New-Item -HypervisorConnectionName MyConnectionName -NetworkPath
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
@($NetworkPath) -Path @($HostingUnitPath) -RootPath $RootPath
-StoragePath @()
```

2. Create an MCS Catalog in an Extended Zone

   After creating your Hosting Unit, proceed with catalog creation using Studio or PowerShell. Ensure your catalog references the Extended Zone Hosting Unit.

Troubleshooting

If you encounter issues, check the following:

1. Ensure your subscription is registered for extended zones.
   a. Confirm your subscription is registered with the Microsoft.EdgeZones resource provider.
   b. Ensure that each Extended Zone is registered individually.
2. Verify your service principal has the new permission.
   a. Your service principal must have the `Microsoft.EdgeZones/extendedZones/read` permission.

Inventory items in Extended Zones may be shown as "Unknown Extended Zone" if registration or permissions are missing.

NOTE:

If creating a catalog in the parent region using a master image from an Extended Zone, registration and permissions for the Extended Zone are still required.

Use a pre-created network security group

Create a Deny-All network security group for image preparation instead of requesting Citrix to create and modify NSG. Edit the custom properties of the hosting unit using a PowerShell command `Set-Item` to include the parameter `NsgForPreparation` to provide the Deny-All network security group.

Prerequisites

Configure the following permissions required for a service principal:

- `Microsoft.Network/networkSecurityGroups/join/action`: Associate a network security group to a subnet or network interface

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Microsoft.Network/networkSecurityGroups/read`: Gets network security group
- `Microsoft.Network/networkSecurityGroups/securityRules/read`: Gets rule

Add the pre-created Deny-All network security group

To add the pre-created Deny-All network security group, set the custom properties as follows on the hosting unit:

1. Open a PowerShell window using the Remote PowerShell SDK.
2. Run the following commands:

```
Add-PSSnapin citrix*.

cd XDHyp:\HostingUnits\

Dir
```

3. Select a hosting unit to retrieve the details:

```
Get-Item "XDHyp:\HostingUnits\<hostingunitname>"
```

4. Copy the CustomProperties to a notepad and append property setting `<Property xsi:type="StringProperty` " Name= `"NsgForPreparation` " Value= `"{ResourceGroupName}/{NetworkSecurityGroupName}"/>`. For example:

```
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>
```

5. In the PowerShell window, assign a variable to the modified custom properties. For example:

```
$customProperty = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Run `$cred = Get-Credential`. If prompted, provide the connection credentials. The credentials are Azure Application ID and secret.
7. Run the following command.

```
Set-Item -PSPath XDHyp:\HostingUnits\<hostingunitname>
-CustomProperties $customProperty -username $cred.username
-Securepassword $cred.password
```

IMPORTANT:

If you get a message stating SubscriptionId is missing, then replace all double quotes (“) with backtick followed by double quotes (`”) in the custom property.

8. Run `dir` to verify the updated `CustomProperties` settings.

NOTE:

It takes more than a minute for the updates to reflect.

Retrieve network security group details

To retrieve the network security group details, first retrieve the resource groups containing the network security group, and then retrieve the network security group based on the resource group name.

1. Retrieve the resource groups containing network security group. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes":
["networksecuritygroup"]}'
```

2. Retrieve the network security group based on the resource group name. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType securitygroup -MaxRecords
5 -AdditionalDataFilter '{"location": ["eastus", "westus"],
"resourcegroup":["resourcegroupname"]}'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filter empty resource groups

Use the PowerShell command `Get-HypInventoryItem` to filter empty resource groups while selecting a master image, machine profile, or prepared image during the machine catalog creation.

Examples:

- Retrieve the maximum records in a page:

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- Retrieve the maximum records in a page, and filter to find resource containers that have specific resources.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- Retrieve with skip to directly indicate the page, and filter to find resource containers that have specific resources.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -skip 20 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- Use a token to retrieve the next page, and filter to find resource containers that have specific resources.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
-ContinuationToken
'ew0KICAiJGlkIjogIjEiLA0KICAiTWF4Um93cyI6IDUsDQogICJSb3dzVG9Ta2lwIjogMj
UsDQogICJLdXN0b0NsdXN0ZXJVcmwiOiAiaHR0cHM6Ly9hcmctbmV1LTEzLXNmLmFyZy5jb
3JlLndpbmRvd3MubmV0Ig0KfQ=='
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Retrieve all resource groups with tag Citrix internal tag and limit max records with `MaxRecords`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- Filter for machine profile (master image) with tag Citrix internal tag and limit max records with `MaxRecords`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- Filter for Prepared image with tag Citrix internal tag and limit max records with `MaxRecords`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion"]}'
```

- Filter for machine profile (Prepared image) with tag Citrix internal tag and limit max records with `MaxRecords`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- Filter for Image with tag Citrix internal tag and limit max records with `MaxRecords` and location.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"], "location": ["eastus",
"westus"]}'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Retrieve all resource group without consideration on tags `CitrixResource`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
50 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"]}' -Force $true
```

Required Azure permissions

This section details the minimum permissions and general permissions required for Azure.

Minimum permissions

Minimum permissions give better security control. However, new features that require additional permissions fail if only minimum permissions are given. This section lists minimum permissions by action.

CREATING A HOST CONNECTION

Add a host connection using the information obtained from Azure.

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/tenants/read",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read",

"Microsoft.EdgeZones/extendedZones/read"
```

POWER MANAGEMENT OF VMS

Power on or off the machine instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

CREATING, UPDATING, OR DELETING VMS

Create a machine catalog, then add, delete, update machines, and delete the machine catalog.

Following is the list of minimum permissions required when the master images are managed disks or snapshots that are in the same region as the hosting connection.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Features/providers/features/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read",

"Microsoft.Compute/capacityReservationGroups/deploy/action"
```

You need the following extra permissions based on minimal permissions for the following features:

- If the master image is a VHD in a storage account in the same region as the hosting connection:

  ```
  "Microsoft.Storage/storageAccounts/read",

  "Microsoft.Storage/storageAccounts/listKeys/action",
  ```

- If the master image is an ImageVersion from the Azure Compute Gallery (formerly Shared Image Gallery):

  ```
  "Microsoft.Compute/galleries/read",

  "Microsoft.Compute/galleries/images/read",

  "Microsoft.Compute/galleries/images/versions/read",
  ```

- If the master image is a managed disk, snapshot, or VHD is in a region different from the region of the hosting connection:

  ```
  "Microsoft.Storage/storageAccounts/read",

  "Microsoft.Storage/storageAccounts/listKeys/action",

  "Microsoft.Storage/storageAccounts/write",

  "Microsoft.Storage/storageAccounts/delete",
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

- If you use the Citrix-managed resource group:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- If you put the master image in Azure Compute Gallery (formerly Shared Image Gallery) in a shared tenant or subscription:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Resources/subscriptions/read",
```

- If you use Azure dedicated host support:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Compute/hostGroups/hosts/read",
```

- If you use Server Side Encryption (SSE) with Customer-Managed Keys (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- If you deploy VMs using ARM templates (machine profile):

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",
```

- If you use Azure template spec as a machine profile:

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

CREATING, UPDATING, AND DELETING MACHINES WITH UNMANAGED DISK

Following is the list of minimum permissions required when the master image is VHD and use resource group as provided by admin:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Network/locations/usages/read"
```

COST MANAGEMENT

Following is the minimum permission required to retrieve VM pricing:

```
"Microsoft.Consumption/pricesheets/read"
```

Following is the minimum permission required to retrieve VM cost:

```
"Microsoft.CostManagement/query/read"
```

NOTE:

To view the **Cost Insights** tab for an Azure machine catalog, you must have **Cost Management > Manage > Read cost** permission (default for Cloud Administrators). For information on **Cost Insights** tab, see View catalog details.

General permissions

Contributor role has full access to manage all resources. This set of permissions does not block you from getting new features.

The following set of permissions provides the best compatibility going forward although it does include more permissions than needed with the current feature set:

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read",

"Microsoft.Consumption/pricesheets/read",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read",

"Microsoft.Compute/capacityReservationGroups/deploy/action",

"Microsoft.EdgeZones/extendedZones/read"
```

Configure required Azure host connection permissions

You can easily configure all the minimum permissions required for a service principal or user account in Azure tied to a host connection to perform all MCS operations using an ARM template. This ARM template automates the following:

- Creation of an Azure Role with minimal permissions necessary for operations.
- Assignment of this role to an existing Azure Service Principal at the subscription level.

You can deploy this ARM template using the Azure Portal or PowerShell commands. For more information, see ARM Template for Citrix Virtual Apps and Desktops Operations.

Validate permissions on host connection

You can validate permissions on a host connection to do tasks related to creating and managing MCS machine catalogs. This implementation helps you to find out the missing permissions required for different scenarios such as creating, deleting, and updating VMs, power management of VMs, ahead of time so that you can avoid being blocked at critical times.

You can validate the permissions on a host connection using the PowerShell command `Test-HypHypervisorConnection`. The result from the command is captured as a list where each item in the list is broken into three sections.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Category: The action or task a user can do to create and manage an MCS machine catalog.
- Corrective Action: The step an admin must do to resolve a users' missing permissions discrepancy.
- Missing permission: The list of missing permissions for a category.

To validate the permissions, do the following:

1. Create a host connection to Azure.
2. Open a PowerShell window from the Delivery Controller™ host.
3. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
4. Run the following command to verify if you have the required permissions to test a connection.

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AzureCon"
   ```

   Role level permission required for the SPN:

   - Microsoft.Authorization/roleDefinitions/read (at subscription level or the resource group level if resource group is provided)
   - Microsoft.Authorization/roleAssignments/read (at subscription level or the resource group level if resource group is provided)

   API level permissions required for the SPN:

   Microsoft.Graph:

   - Application.Read.All
   - Directory.Read.All
   - ServicePrincipalEndpoint.Read.All

5. After you add the missing permissions required to look up your permissions, run the following command to verify if you have permissions in the various categories.

   Example:

   To test a connection at the subscription level with a higher level of authorization required:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\ AzureCon
   -SecurePassword $password -UserName 922e65d5-38ae-4cf5-xxxx-xxxxxxxxx
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example:

To test a connection at the resource group level without a high level of authorization:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-CustomProperties $customProperties | Format-List
```

NOTE:

The `CustomProperties` parameter is used to provide the resource group level because resource group is a connection specific information.

Example:

To test a connection with the higher level of authorization at resource group level:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-SecurePassword $password -UserName
922e65d5-38ae-4cf5-832b-54122196b7dd -CustomProperties
$customProperties
```

For information on permissions, see Required Azure permissions.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For Azure-specific information, see Create a Microsoft Azure catalog.

More information

- Create and manage connections and resources
- Microsoft Azure Resource Manager virtualization environments

Connection to Microsoft SCVMM

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Microsoft System Center Virtual Machine Manager (VMM).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Before creating a connection to VMM, you need to first finish setting up your VMM as a resource location. See Microsoft System Center Virtual Machine Manager virtualization environments.

Create a connection

If you used MCS to provision VMs, do the following in the connection creation wizard:

- Enter the address as a fully qualified domain name of the host server.
- Enter the credentials for the administrator account that you set up earlier. This account must have permission to create new VMs.
- In the Host Details dialog box, select the cluster or standalone host to use when creating VMs.

IMPORTANT

Browse for a cluster or standalone host even if you are using a single Hyper-V host deployment.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For creating machine catalogs with MCS on SMB 3 file share, see Create a Microsoft System Center Virtual Machine Manager catalog.

More information

- Create and manage connections and resources
- Microsoft System Center Virtual Machine Manager virtualization environments.

Connection to Nutanix

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Nutanix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Before creating a connection to Nutanix, you need to first finish setting up your Nutanix account as a resource location. See Nutanix virtualization environments.

Nutanix AHV Prism Central host connection

See the Prerequisites before creating Nutanix AHV Prism Central host connection.

You can create a connection using one of the following:

- Studio
- PowerShell commands

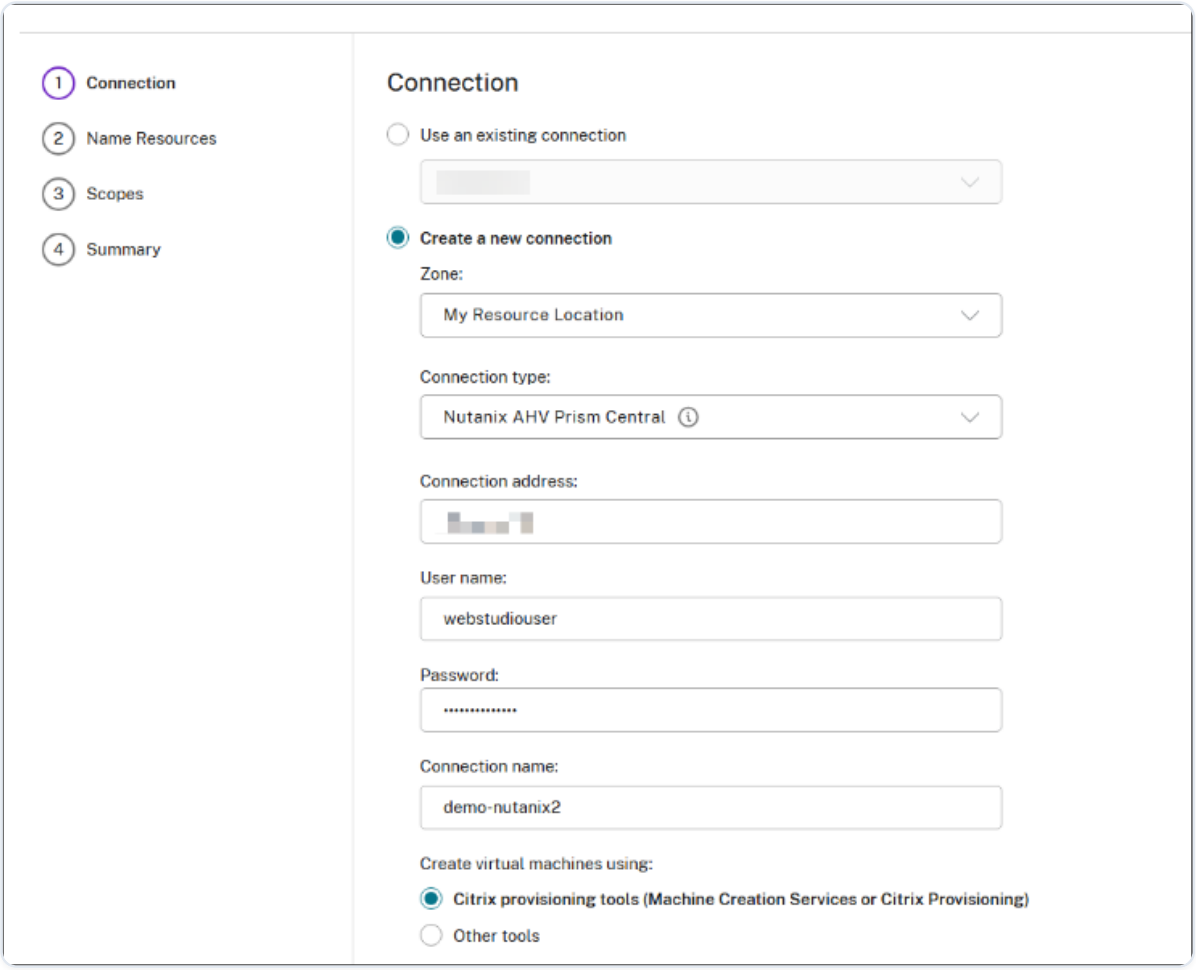
Limitation

- The Nutanix AHV Prism Central host connection doesn't support duplicate object names for items such as templates and networks. Selecting such items for catalog creation might lead to unexpected behavior.

Create a connection using Studio

1. Sign in to Citrix Cloud.
2. In the DaaS tile, click **Manage**.
3. Select **Hosting** in the left pane.
4. Click **Add Connections and Resources** in the action bar.
5. On the **Connection** page:
    a. Select **Create a new connection**.
    b. Select **Nutanix AHV Prism Central** as the connection type.
    c. Enter the IP address of your Nutanix AHV Prism Central as the connection address.
    d. Enter your administrative credentials and a friendly connection name.
    e. Select **Citrix provisioning tools (Machine Creation Services™ or Citrix Provisioning)**.
    f. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



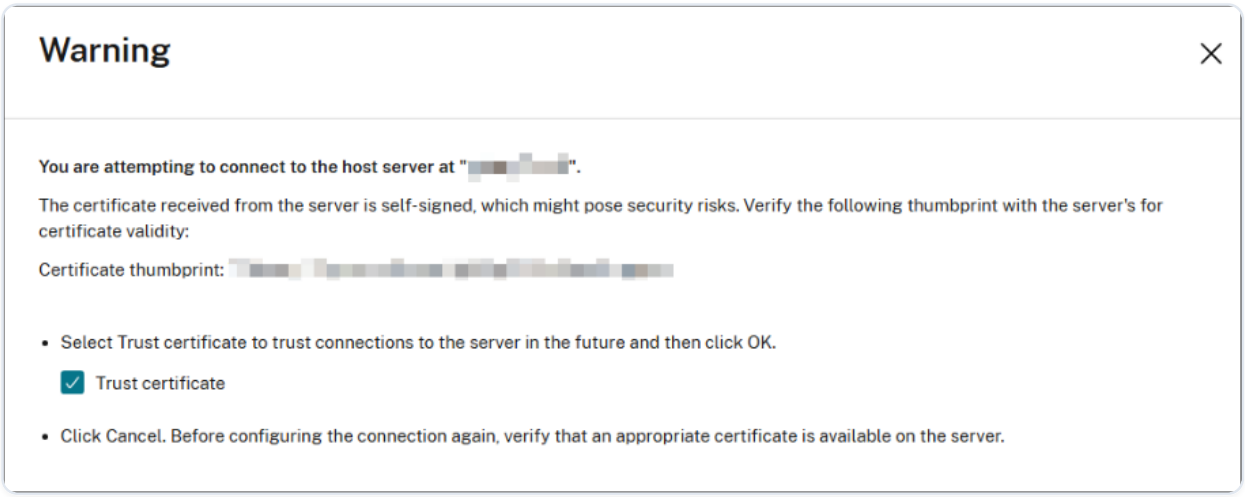
NOTE:

While creating the host connection, network or cluster selection is not required. A hosting unit name is only needed. Select the network and cluster while creating the machine catalog.

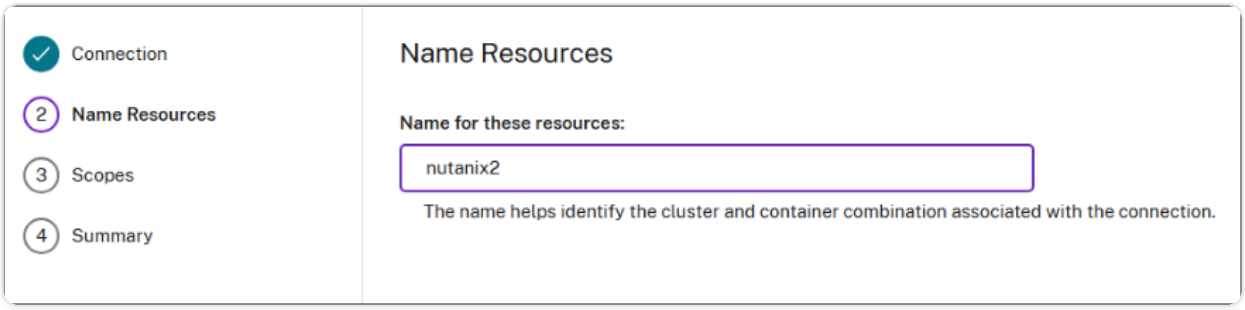
6. After you click **Next**, Citrix DaaS™ receives a private CA-signed certificate and you see a **Warning** page. For information, see Secure connections to the Nutanix Prism Central.

   Compare the received thumbprint with the server's for the certificate validity. If it's valid, select **Trust certificate** and click **OK** to proceed with connection creation. Citrix DaaS then trusts the certificate and stores the thumbprint for future validation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. On the **Name Resources** page, add a unique name of the resources. Click **Next**.



8. On the **Scopes** page, select one or more scopes for this host.
9. On the **Summary** page, check the configuration and click **Finish**.

NOTE:

The Nutanix AHV Prism Central connection can co-exist with other types of Nutanix connections.

Secure connections to the Nutanix Prism Central

The Nutanix SSL thumbprint feature simplifies certificate trust when establishing a host connection to a Nutanix Prism Central hypervisor. This feature enables the storage of an untrusted certificate's thumbprint in the site database, ensuring that Citrix DaaS consistently recognizes the hypervisor as trusted.

When creating a Nutanix host connection, a **Warning** page is displayed, presenting the certificate of the machine you are connecting to and allowing you to decide whether to trust it.

Create a connection using PowerShell

1. Open the PowerShell window.
2. Run `asnp citrix*`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Set following parameters:

```
$ConnectionName = “Name of the connection”

$UserName = “Username of the account on hypervisor”

$ZoneUid =  “UID of the zone where the hosting connection will be
created”

$HypervisorAddress = “The IP address of the hypervisor”

$SSLThumbprint =  “The Nutanix PC SSL thumbprint can be set using
PowerShell SDK”

$connectionPath = "XDHyp:\Connections\" + $ConnectionName

$SecureUserInput = Read-Host "Enter the password for the user $
($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput
```

4. Create an item for the new hosting connection. For example:

```
$connection = New-Item -Path @($connectionPath) -ConnectionType
"Custom" -HypervisorAddress ` @($HypervisorAddress) -Persist -PluginId
"AcropolisHypervisorPCFactory" -Scope @() ` -SecurePassword $SecurePass
-SSLThumbprint @($SSLThumbprint) -UserName $UserName -ZoneUid `
$ZoneUid
```

5. Create a broker hypervisor connection. For example:

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

CREATE A HOSTING UNIT

When you create a hosting unit using the PowerShell command, provide the following required parameters:

- `$HostUnitName`: Name of Hosting Unit to create

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `ConnectionName`: Name of the hypervisor connection previously created

1. Open the PowerShell window.
2. Run `add-pssnapin citrix*`.
3. Run PowerShell commands to create the hosting unit. For example:

```
$hostUnitPath = "XDHyp:\HostingUnits\" + $HostUnitName

New-Item -Path @($hostUnitPath) -RootPath $connectionPath
-HypervisorConnectionName $ConnectionName -CustomProperties ""
-NetworkPath @() -StoragePath @()
```

NOTE:

While creating the host connection, network or cluster selection is not required. A hosting unit name is only needed. Select the network and cluster while creating the machine catalog.

Manage host connections

You can manage an exisiting host connection using:

- Studio
- PowerShell

MANAGE THE HOST CONNECTION USING STUDIO

After creating a host connection, navigate to the **Hosting** node on Studio and right-click a connection to do the following:

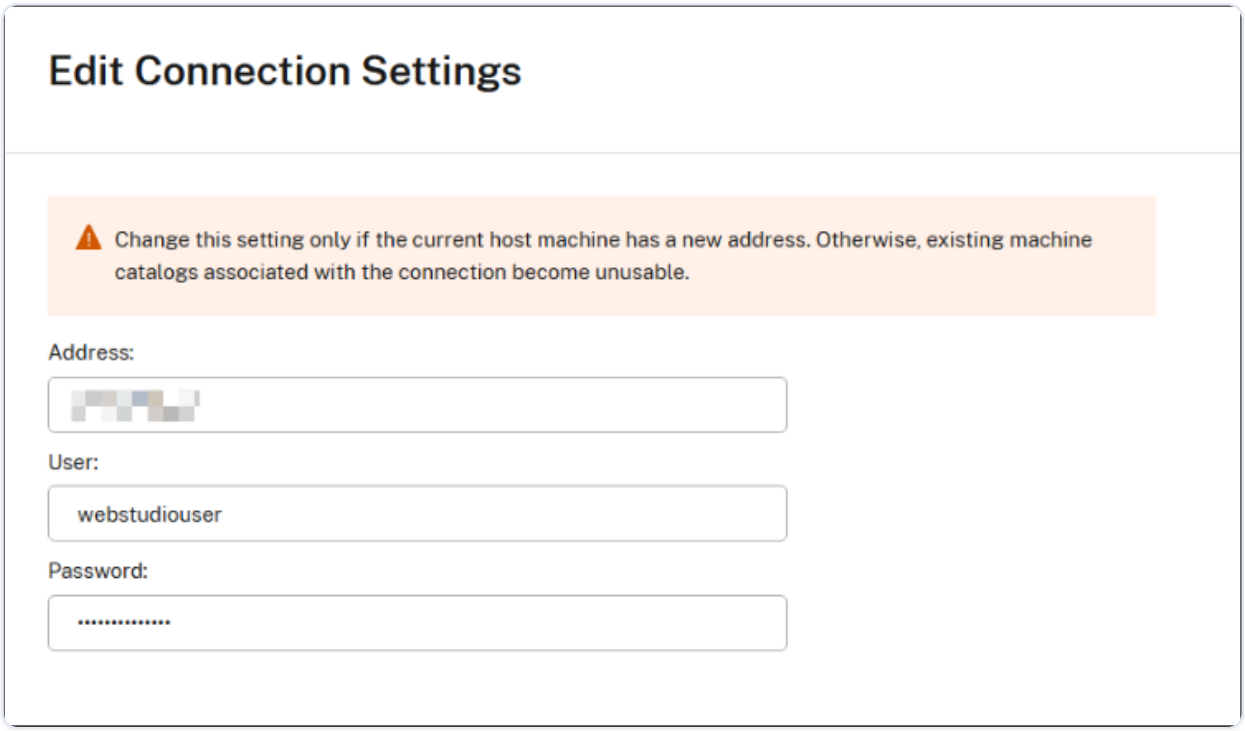
- **Delete Connection**
- **Rename Connection**
- **Edit Connection**
- **Turn on Maintenance Mode**
- **View Machines**
- **Test Connection**
- **Test TLS certificate trust**

EDIT A CONNECTION USING STUDIO

1. Right-click a connection and click **Edit Connection**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the **Connection Properties** page, click **Edit settings**.
3. On the **Edit Connection settings** page, you can change the certificate information and click **Save**.

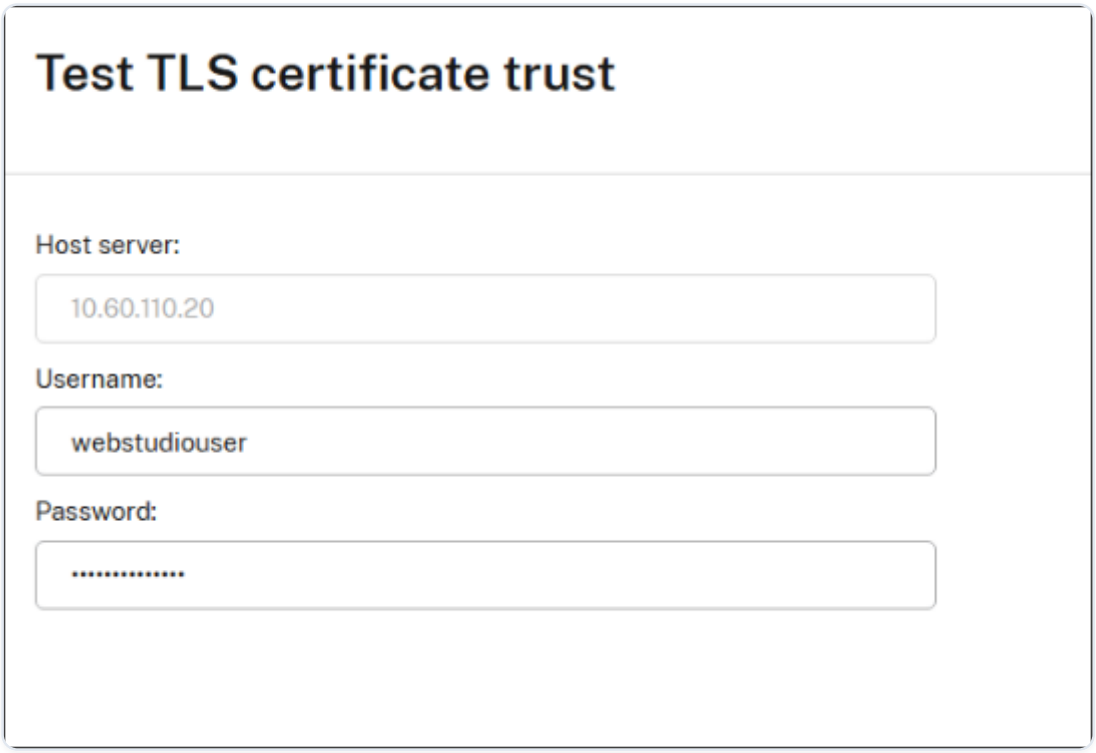


4. Select **Trust certificate** on the **Warning** page to trust the new certificate thumbprint.

TEST TLS CERTIFICATE TRUST

1. Right-click a connection and click **Test TLS certificate trust**.
2. On the **Test TLS Certificate Trust** page, you can change the certificate information, then click **Test**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If the test result is not successful, then change the certificate information of the connection using Edit a connection using Studio.

MANAGE THE HOST CONNECTION USING POWERSHELL

You can use PowerShell commands to:

- Change or update the user credential for a host connection. For example:

```
$UserName = "Username of the account on hypervisor"

$SecureUserInput = Read-Host "Enter the password for the user $
($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
 -SecurePassword $SecurePass -UserName $UserName
```

- Reset SSLThumbprint. For example:

```
$SSLThumbprint =  "The Nutanix PC SSL thumbprint value"

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 -SecurePassword $SecurePass -UserName $UserName -SSLThumbprint
$SSLThumbprint
```

Required permissions

The following permissions are required for the administrative account used for a Nutanix AHV Prism Central host connection.

CREATING A HOST CONNECTION

Cluster:

- View Cluster

POWER MANAGEMENT OF VMS

AHV VM:

- ACPI Shutdown Virtual Machine
- ACPI Reboot Virtual Machine
- Guest Reboot Virtual Machine
- Guest Shutdown Virtual Machine
- Power Off Virtual Machine
- Power On Virtual Machine
- Reset Virtual Machine
- View Existing Virtual Machine

Cluster:

- View Cluster

Subnet:

- View Subnet

PROVISIONING OF VMS

AHV VM:

- ACPI Reboot Virtual Machine
- ACPI Shutdown Virtual Machine
- Associate Virtual Machine Categories
- Create New Virtual Machine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Create Virtual Machine
- Create Virtual Machine Disk
- Create Virtual Machine NIC
- Delete Existing Virtual Machine
- Delete Virtual Machine
- Delete Virtual Machine Disk
- Delete Virtual Machine GPU
- Delete Virtual Machine NIC
- Disassociate Virtual Machine Categories
- Eject Virtual Machine CD ROM
- Guest Reboot Virtual Machine
- Guest Shutdown Virtual Machine
- Power Off Virtual Machine
- Power On Virtual Machine
- Reset Virtual Machine
- Snapshot Virtual Machine
- Update Virtual Machine Basic Config
- Update Virtual Machine Disk
- Update Virtual Machine Disk List
- Update Virtual Machine NIC
- View Existing Virtual Machine
- View Virtual Machine
- View Virtual Machine CD ROM
- View Virtual Machine Disk
- View Virtual Machine GPU
- View Virtual Machine NIC

AHV VM Recovery Point:

- View AHV VM Recovery Point

Category:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- View Category

Cluster:

- View Cluster

Host:

- View Host

Image:

- Create Image
- Delete Image
- Update Image
- View Image

Recovery Point:

- Create Recovery Point
- Delete Recovery Point
- Replicate Recovery Point
- Restore Recovery Point
- View Recovery Point
- View Virtual Machine Recovery Point

Storage Container:

- View Storage Container
- View Storage Container Datastore
- View Storage Container Stats

Storage Policy:

- View Storage Policy

Subnet:

- View Subnet
- View Subnet Vnic

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Task:

- Cancel Task
- View Task

VM Recovery Point:

- Delete VM Recovery Point
- Restore VM Recovery Point
- View VM Recovery Point

VM Templates:

- View VM Templates
- View VM Templates Versions
- Deploy VM Templates

Volume Group:

- Attach Volume Group To AHV VM
- Detach Volume Group From AHV VM
- View Volume Group
- View Volume Group Details

VPC:

- View VPC

Nutanix AHV, Nutanix AHV PC, or Nutanix AHV DRaaS host connection

1. Sign in to Citrix Cloud.
2. In the DaaS tile, click **Manage**.
3. Select **Hosting** in the left pane.
4. Click **Add Connections and Resources** in the action bar.
5. On the **Connection** page, the following connection types are available for selection:

    - **Nutanix AHV**: specify the Prism Element (PE) cluster address, and credentials, and a name for the connection. On the **Network** page, select network(s) and give a name for the hosting unit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> If you deploy machines using Nutanix AHV (Prism Element) as the resource, select the container where the VM's disk resides.

- **Nutanix AHV PC**: specify the Prism Central (PC) address, credentials, and a name for the connection. On the **Network** page, select the network, cluster from the list, and give a name for the hosting unit.

  > **NOTE:**
  >
  > The connection type **Nutanix AHV PC** is only used for creating connection to Nutanix Cloud Cluster (NC2) on Azure. Also, a machine catalog can only be hosted on a single cluster in an NC2 on Azure connection. This type of connection requires a Nutanix plug-in installed on Cloud Connectors

- **Nutanix AHV DRaaS**: specify your address and user name, and then import the public and private keys contained in your Nutanix DRaaS credential files `.pem`. (Public and private keys are generated in Nutanix DRaaS cloud by Nutanix DRaaS administrators.)

  - To import the key, locate your credential file, open it with Notepad (or any text editor), and then copy the content. After that, return to the **Connection** page, select **Import key**, paste the content, and then select **Save**. Do not change the credential content or its format.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For Nutanix specific information, see Create a Nutanix catalog.

More information

- Create and manage connections and resources
- Nutanix virtualization environments
- Nutanix cloud and partner solutions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connection to Nutanix cloud and partner solutions

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Nutanix cloud and partner solutions.

Nutanix AHV Prism Central

Citrix DaaS™ supports Nutanix Cloud Clusters (NC2) in the following cloud hypervisors for Citrix-managed Nutanix AHV Prism Central plug-in.

- AWS
- Microsoft Azure

NOTE:

- Before creating a connection to NC2 on AWS and Azure, prepare the resources in the cloud platform. See Nutanix cloud and partner solutions.
- For the permissions to create hosting connection, power management of VMs, and provisioning of catalogs, see Required permissions.

Connect to NC2 on Azure and AWS

Connecting to a Nutanix Cloud Cluster (NC2) on Azure or AWS requires access to a deployed Prism Central instance and credentials with the Prism Admin role.

You can create a host connection using:

- Studio
- PowerShell

For the complete information on connection, see Connection to Nutanix AHV Prism Central

Nutanix Prism Element

Citrix DaaS supports Nutanix Cloud Clusters (NC2) in the following cloud hypervisor for the Nutanix Prism Element plug-in.

- AWS

Connect to Nutanix Prism

After you create a Nutanix cluster, connect to Nutanix Prism. To connect to Nutanix Prism:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Create a bastion VM in the 10.0.129.0/24 subnet.
2. RDP into the bastion VM, go to the URL of the **Prism Element** you copied in the previous section.
3. Log in using the default credentials: `admin:nutanix/4u`. Remember to change the password.

Create a VM on the Nutanix Cluster

After connecting to **Nutanix Prism**, create VMs on the Nutanix cluster.

IF THE VM NEEDS INTERNET ACCESS

1. Go to the AWS console.
2. Create a new subnet 10.0.130.0/24 in the same VPC as the one created by Nutanix CFS.
3. Add a route to the route table of this subnet to direct all none local traffic to the NAT gateway above.
4. RDP into the bastion VM, go to the URL of the **Prism Element** you copied in the previous section and login.
5. Add a new network. Go to **Settings>Network Configuration>Create Subnet**. Use the same subnet 10.0.130.0/24 used in AWS.
6. Create all the VMs (AD, CC, VDA, and so on) in that new subnet.

IF THE VM DOES NOT NEED INTERNET ACCESS

1. RDP into the bastion VM, go to the URL of the **Prism Element** you copied in the previous section and login.
2. Add a new network. Go to **Settings>Network Configuration>Create Subnet**. Use the subnet 10.0.129.0/24.
3. Create all the VMs (AD, CC, VDA, and so on) in that subnet.

TIP:

Make sure that the time and timezone information in the VMs are set up correctly. This is especially true for AD.

Create host connection

1. From Studio, select **Hosting** in the left pane.
2. Click **Add Connection and Resources**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Connection** screen, select **Create a new Connection**, and in the **Connection address**, enter `https://xxx.xxx.xxx.xxx:9440`.
4. Follow the UI to complete the wizard.

NOTE:

All connector VMs must have the Nutanix plug-in installed for the Nutanix option to be available in Citrix Studio, even if the plug-ins are not used in the Nutanix zone.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For Nutanix specific information, see Create a Nutanix catalog.

More information

- Create and manage connections and resources
- Nutanix virtualization environments
- Nutanix cloud and partner solutions

Connection to Red Hat OpenShift

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Red Hat OpenShift.

NOTE:

Before creating a connection to Red Hat OpenShift, you need to first finish setting up your Red Hat OpenShift. See Red Hat OpenShift virtualization environments.

Create a connection

You can create a connection to the Red Hat OpenShift cluster using:

- Studio
- PowerShell

Create a connection using Studio

1. Navigate to **Hosting > Add Connection and Resources**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the **Connection** page, follow these steps to configure the connection:

    a. Select **Create a new connection**.

    b. Select **Red Hat OpenShift** as the Connection type.

    c. In the **Connection address** field, enter the IP address, hostname, or FQDN of the OpenShift Server.

    d. Enter your service account token and a friendly connection name.

    e. Select a zone in the **Zone name** field. The options are all resource locations you configured.

    f. Select **Other tools** for creating virtual machines.

    > **NOTE:**
    >
    > Selecting **Other tools** creates just the hosting connection without a hosting unit.

3. Click **Next**.
4. If a self-signed certificate is detected, a warning page appears with the certificate thumbprint. To proceed:

    a. Compare the thumbprint with the server's to verify the certificate's validity.

    b. If valid, select **Trust certificate** and click **OK** to complete the connection setup.

    The certificate is marked as trusted, and the thumbprint is saved for future validation.

5. On the **Scopes** page, select one or more scopes for this host.
6. On the **Summary** page, check the configuration and click **Finish**.

Create a connection using PowerShell commands

When you create a connection using PowerShell command, provide the following information:

- Hosting connection name
- Cluster API address
- User name
- Password (Service account token)
- SSLThumbprint: This is a CA Cert thumbprint and not the API server thumbprint. The server provides the CA Cert thumbprint if you try to create a hosting connection without specifying the thumbprint.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ZoneUid

1. Open the PowerShell window.
2. Run `add-pssnapin citrix*`.
3. Run the following command to create the hosting connection.

   If you try to create a hosting connection without specifying the thumbprint, then the server provides the CA Cert thumbprint. For example:

```
$newItemParameters = @{

ConnectionType= "Custom"

PluginId= "OpenShiftPluginFactory"

HypervisorAddress = "https://
api.myopenshiftclusteraddress.mydomain.local:6443"

Path= "XDHyp:\Connections\OpenShiftConnectionName"

Persist= $true

UserName= "__ServiceAccount__"

Password= "<service account token>"

ErrorVariable= "connectionError"

 }



& New-Item @newItemParameters




$newItemParameters["SSLThumbprint"] =
$connectionError[0].ErrorData.Thumbprint

$connection = & New-Item @newItemParameters
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$brokerConnection = New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```

Create a hosting unit

A hosting unit represents an environment where VMs are created. To create the hosting unit, you need the following inputs from OpenShift:

- Namespace
- StorageClasses
- Network Attachment Definition

A hosting unit is a namespace-bound. This means that one hosting unit can access only one namespace and manages the VMs under the namespace.

You can create a hosting unit using:

- Studio
- PowerShell

Create hosting units using Studio

1. Navigate to **Hosting > Add Connection and Resources**.
2. On the **Connection** page:
    - To create a new hosting connection along with a hosting unit, select **Create a new connection**, then do the following:
        a. Select **Red Hat OpenShift** as the Connection type.
        b. In the **Connection address** field, enter the IP address, hostname, or FQDN of the OpenShift Server.
        c. Enter your service account token and a friendly connection name.
        d. Select a zone in the **Zone name** field. The options are all resource locations you configured.
        e. Select **Citrix provisioning tools (Machine Creation Services™ or Citrix Provisioning) for creating virtual machines**.
        f. Click **Next**.
        g. On the **Warning** page, verify the certificate's validity, and select **Trust certificate**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To create hosting units from an existing host connection, select **Use an existing Connection** and then choose the relevant connection.

3. On the **Namespace Selection** page, select a namespace for this connection.
4. On the **Storage Selection** page, select at least one storage device for each supported data type before you can proceed to the next page in the wizard. For more information about storage selection, see Host storage.
5. On the **Network** page, enter a name for the resources. This name appears in Studio to identify the storage and network combination associated with the connection. Select one or more networks that the VMs use.
6. On the **Summary** page, check the details and click **Finish**.

Create hosting units using PowerShell

When you create a hosting unit using PowerShell command, provide the following information:

- A hosting connection name
- A hosting unit name
- The target namespace name
- A StorageClasses name
- A NetworkAttachmentDefinition name

1. Open the PowerShell window.
2. Run `add-pssnapin citrix*`.
3. Run PowerShell commands to create the hosting unit. For example:

```
$HostingConnectionName = "OpenShiftConnectionName"

$HostingUnitName = "HostingUnitName"

$TargetNamespace = "TargetNamespaceName"

$StorageClassToUse = "YourStorageClassesName"

$NetworkAttachmentDefinition = "YourNetworkAttachmentDefinitionName"

New-HypStorage `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$TargetNamespace.namespace\$StorageClassToUse.storage") `

-StorageType "TemporaryStorage"

New-Item `

-CustomProperties "" `

-HypervisorConnectionName $HostingConnectionName `

-NetworkPath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$NetworkAttachmentDefinition.network") `

-Path @("XDHyp:\HostingUnits\$HostingUnitName") -RootPath "XDHyp:
\Connections\$HostingConnectionName\$TargetNamespace.namespace" `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage")
```

Where to go next

- If you're in the initial deployment process, see Create machine catalogs
- For Red Hat OpenShift specific information, see Create a Red Hat OpenShift catalog

More information

- Connections and resources
- Red Hat OpenShift virtualization environments

Connection to VMware

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to VMware virtualization environments.

NOTE:

Before creating a connection to VMware, you need to first finish setting up your VMware account as a resource location. See VMware virtualization environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Required permissions

Create a VMware user account and one or more VMware roles with a set or all permissions listed in this article. Base the roles' creation on the specific level of granularity required over the user's permissions to request the various Citrix DaaS™ operations at any time. To grant the user-specific permissions at any point, associate them with the respective role, at the data center level at a minimum, with the **Propagate to children** option selected. However, for `StorageProfile` permissions and a specific `Tags` permission, apply the permissions at the Root vCenter Server level, without **Propagate to Children**. See the notes in each of those tables.

The following tables show the mappings between Citrix DaaS operations and the minimum required VMware permissions.

Add connections and resources

SDK	USER INTERFACE
System. Anonymous, System. Read, and System.View	Added automatically. Can use the built-in read-only role.

Power management

SDK	USER INTERFACE
VirtualMachine.Interact.PowerOff	**Virtual machine > Interaction > Power Off**
VirtualMachine.Interact.PowerOn	**Virtual machine > Interaction > Power On**
VirtualMachine.Interact.Reset	**Virtual machine > Interaction > Reset**
VirtualMachine.Interact.Suspend	**Virtual machine > Interaction > Suspend**
Datastore.Browse	**Datastore > Browse datastore**

Provision machines (Machine Creation Services™)

To provision machines using MCS, the following permissions are mandatory:

SDK	USER INTERFACE
Datastore.AllocateSpace	**Datastore > Allocate space**
Datastore.Browse	**Datastore > Browse datastore**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDK	USER INTERFACE
Datastore.FileManagement	**Datastore > Low level file operations**
Network.Assign	**Network > Assign network**
Resource.AssignVMToPool	**Resource > Assign virtual machine to resource pool**
VirtualMachine.Config.AddExistingDisk	**Virtual machine > Configuration > Add existing disk**
VirtualMachine.Config.AddNewDisk	**Virtual machine > Configuration > Add new disk**
Virtual machine.Config.Add or remove device	**Virtual machine > Configuration > Add or remove device**
VirtualMachine.Config.AdvancedConfig	**Virtual machine > Configuration > Advanced**
VirtualMachine.Config.RemoveDisk	**Virtual machine > Configuration > Remove disk**
VirtualMachine.Config.CPUCount	**Virtual machine > Configuration > Change CPU count**
VirtualMachine.Config.Memory	**Virtual machine > Configuration > Change memory**
VirtualMachine.Config.Settings	**Virtual machine > Configuration > Change settings**
VirtualMachine.Interact.PowerOff	**Virtual machine > Interaction > Power Off**
VirtualMachine.Interact.PowerOn	**Virtual machine > Interaction > Power On**
VirtualMachine.Interact.Reset	**Virtual machine > Interaction > Reset**
VirtualMachine.Interact.Suspend	**Virtual machine > Interaction > Suspend**
VirtualMachine.Inventory.CreateFromExisting	**Virtual machine > Inventory > Create from existing**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDK	USER INTERFACE
VirtualMachine.Inventory.Create	**Virtual machine > Inventory > Create new**
VirtualMachine.Inventory.Delete	**Virtual machine > Inventory > Remove**
VirtualMachine.Provisioning.Clone	**Virtual machine > Provisioning > Clone virtual machine**
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1, and vSphere 6.x, Update 1: **Virtual machine > State > Create snapshot**; vSphere 5.5: **Virtual machine > Snapshot management > Create snapshot**; vSphere 8.0: **Virtual machine > Snapshot management > Create snapshot**
VirtualMachine.Config.Rename	**Virtual machine > Configuration > Rename**

Image update and rollback

SDK	USER INTERFACE
Datastore.AllocateSpace	**Datastore > Allocate space**
Datastore.Browse	**Datastore > Browse datastore**
Datastore.FileManagement	**Datastore > Low level file operations**
Network.Assign	**Network > Assign network**
Resource.AssignVMToPool	**Resource > Assign virtual machine to resource pool**
VirtualMachine.Config.AddExistingDisk	**Virtual machine > Configuration > Add existing disk**
VirtualMachine.Config.AddNewDisk	**Virtual machine > Configuration > Add new disk**
VirtualMachine.Config.AdvancedConfig	**Virtual machine > Configuration > Advanced**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDK	USER INTERFACE
VirtualMachine.Config.RemoveDisk	**Virtual machine > Configuration > Remove disk**
VirtualMachine.Interact.PowerOff	**Virtual machine > Interaction > Power Off**
VirtualMachine.Interact.PowerOn	**Virtual machine > Interaction > Power On**
VirtualMachine.Interact.Reset	**Virtual machine > Interaction > Reset**
VirtualMachine.Inventory.CreateFromExisting	**Virtual machine > Inventory > Create from existing**
VirtualMachine.Inventory.Create	**Virtual machine > Inventory > Create new**
VirtualMachine.Inventory.Delete	**Virtual machine > Inventory > Remove**
VirtualMachine.Provisioning.Clone	**Virtual machine > Provisioning > Clone virtual machine**

Share prepared images

To share prepared images across different hosting connections, the following permissions are mandatory for target hosting connection:

SDK	USER INTERFACE
Datastore.AllocateSpace	**Datastore > Allocate space**
Network.Assign	**Network > Assign network**
Resource.AssignVMToPool	**Resource > Assign virtual machine to resource pool**
VirtualMachine.Config.Add or remove device	**Virtual machine > Configuration > Add or remove device**
VirtualMachine.Config.RemoveDisk	**Virtual machine > Configuration > Remove disk**
VirtualMachine.Config.Settings	**Virtual machine > Configuration > Change settings**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDK	USER INTERFACE
VirtualMachine.Inventory.Register	**Virtual machine > Inventory > Register**
VirtualMachine.Inventory.Delete	**Virtual machine > Inventory > Remove**
VirtualMachine.Provisioning.MarkAsTemplate	**Virtual machine > Provisioning > Mark as template**
VirtualMachine.Provisioning.MarkAsVM	**Virtual machine > Provisioning > Mark as virtual machine**
Host.Config.Network	**Host > Configuration > Network configuration**

Delete provisioned machines

SDK	USER INTERFACE
Datastore.Browse	**Datastore > Browse datastore**
Datastore.FileManagement	**Datastore > Low level file operations**
VirtualMachine.Config.RemoveDisk	**Virtual machine > Configuration > Remove disk**
VirtualMachine.Interact.PowerOff	**Virtual machine > Interaction > Power Off**
VirtualMachine.Inventory.Delete	**Virtual machine > Inventory > Remove**

Storage Profile

To view, create, or delete storage policies during catalog creations on a vSAN or vVol datastore, the following permissions are mandatory:

SDK	USER INTERFACE
StorageProfile.Update	**PROFILE-DRIVEN STORAGE > Profile-driven storage update**. For vSphere 8: **VM storage policies > Update VM storage policies**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDK	USER INTERFACE
StorageProfile.View	**PROFILE-DRIVEN STORAGE > Profile-driven storage view**. For vSphere 8: **VM storage policies > View VM storage policies**

NOTE:

Apply the storage profile permissions at the Root vCenter Server level, without **Propagate to Children**.

Tags and Custom Attributes

Tags and custom attributes allow you to attach metadata to the VMs created in vSphere inventory and make it easier to search and filter these objects. To create, edit, assign, and delete tags or categories, the following permissions are mandatory:

SDK	USER INTERFACE
InventoryService.Tagging.CreateTag	**vSphere Tagging > Create vSphere Tag**
InventoryService.Tagging.CreateCategory	**vSphere Tagging > Create vSphere Tag Category**
InventoryService.Tagging.EditTag	**vSphere Tagging > Edit vSphere Tag**
InventoryService.Tagging.EditCategory	**vSphere Tagging > Edit vSphere Tag Category**
InventoryService.Tagging.DeleteTag	**vSphere Tagging > Delete vSphere Tag**
InventoryService.Tagging.DeleteCategory	**vSphere Tagging > Delete vSphere Tag Category**
InventoryService.Tagging.AttachTag	**vSphere Tagging > Assign or Unassign vSphere Tag**
InventoryService.Tagging.ObjectAttachable	**vSphere Tagging > Assign or Unassign vSphere Tag on Object**
Global.ManageCustomFields	**Global > Manage custom attributes**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDK	USER INTERFACE
Global.SetCustomField	**Global > Set custom attribute**

NOTE:

- When MCS creates a machine catalog, it tags the target VMs with special name tags. These tags differentiate the master image from MCS created VMs and prevent using MCS created VMs for image preparation. You can identify the difference by the value of `XdProvisioned` attribute in vCenter. The attribute is set to **True** if MCS creates VMs.
- Apply the `InventoryService.Tagging.AttachTag` permission at the Root vCenter Server level, without **Propagate to Children**.

Cryptographic operations

Cryptographic operations privileges control who can perform which type of cryptographic operation on which type of object. vSphere Native Key Provider uses the `Cryptographer.*` privileges. The following minimum permissions are required for cryptographic operations:

NOTE:

These permissions are required for creating MCS machine catalogs with vTPM equipped VM.

SDK	USER INTERFACE
Cryptographer.Access	**Privileges > All Privileges > Cryptographic operations > Direct Access**
Cryptographer.AddDisk	**Privileges > All Privileges > Cryptographic operations > Add disk**
Cryptographer.Clone	**Privileges > All Privileges > Cryptographic operations > Clone**
Cryptographer.Encrypt	**Privileges > All Privileges > Cryptographic operations > Encrypt**
Cryptographer.EncryptNew	**Privileges > All Privileges > Cryptographic operations > Encrypt new**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDK	USER INTERFACE
Cryptographer.Decrypt	**Privileges > All Privileges > Cryptographic operations > Decrypt**
Cryptographer.Migrate	**Privileges > All Privileges > Cryptographic operations > Migrate**
Cryptographer.ReadKeyServersInfo	**Privileges > All Privileges > Cryptographic operations > Read KMS information**

Provision machines (Citrix Provisioning™)

These permissions to clone and deploy a template are required to provision VMs using Citrix Virtual Apps and Desktops™ Setup Wizard and Export Devices Wizard through the Citrix Provisioning console. Set the permissions while creating a hosting connection. You need all the permissions from Provision machines (Machine Creation Services) and the following.

SDK	USER INTERFACE
VirtualMachine.Config.AddRemoveDevice	**Virtual machine > Configuration > Add or remove device**
VirtualMachine.Config.CPUCount	**Virtual machine > Configuration > Change CPU Coun**t
VirtualMachine.Config.Memory	**Virtual machine > Configuration > Memory**
VirtualMachine.Config.Settings	**Virtual machine > Configuration > Settings**
VirtualMachine.Provisioning.CloneTemplate	**Virtual machine > Provisioning > Clone template**
VirtualMachine.Provisioning.DeployTemplate	**Virtual machine > Provisioning > Deploy template**
VApp.Export	**vApp > Export**

NOTE:

The `VApp.Export` is required for creating MCS machine catalogs using machine profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Securing connections to the VMware environment

Using `HTTPS/SSL` connections to vCenter requires that the connection is trusted by Citrix DaaS.

There are two options:

- (Recommended) The Citrix DaaS database has the SSL thumbprint installed. This thumbprint is used by Citrix DaaS on each Cloud Connector to trust connections to vCenter.
- (Alternative) Each Cloud Connector trusts the vCenter certificate, and services on the Cloud Connector reuses this trust. This trust can be from:
  - vCenter certificate, issued by the Certificate Authority and trusted by windows, resulting in established trust between Windows and vCenter.
  - vCenter certificate installed on Windows, resulting in established trust between Windows and vCenter.OT

NOTE:

vCenter certificate and VMware SSL thumbprint are not required for VMware Cloud and its partner solutions.

VMware SSL thumbprint

The VMware SSL thumbprint feature addresses a frequently reported error when creating a host connection to a VMware vSphere hypervisor. Previously, administrators had to manually create a trust relationship between the Citrix-managed Delivery Controllers in the Site and the hypervisor's certificate before creating a connection. The VMware SSL thumbprint feature removes that manual requirement: the untrusted certificate's thumbprint is stored on the Site database so that the hypervisor can be continuously identified as trusted by Citrix DaaS, even if not by the Controllers.

When creating a vSphere host connection, a dialog box allows you to view the certificate of the machine you are connecting to. You can then choose whether to trust it.

The VMware SSL thumbprint can be updated later using PowerShell SDK `Set-Item -LiteralPath "<FullPath_to_connection>" -username $cred.username -Securepassword $cred.password -SslThumbprint "<New ThumbPrint>" -hypervisorAddress <vcenter URL>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP:

The certificate thumbprint must be written in capital letters.

Obtain and import a certificate

To protect vSphere communications, Citrix® recommends that you use HTTPS rather than HTTP. HTTPS requires digital certificates. Citrix recommends you use a digital certificate issued from a certificate authority in accordance with your organization's security policy.

If you are unable to use a digital certificate issued from a certificate authority, and your organization's security policy permits it, you can use the VMware-installed self-signed certificate. Add the VMware vCenter certificate to each Cloud Connector.

1. Add the fully qualified domain name (FQDN) of the computer running vCenter Server to the host file on that server, located at %SystemRoot%/WINDOWS/system32/Drivers/etc/. This step is required only if the FQDN of the computer running vCenter Server is not already present in the domain name system.
2. Obtain the vCenter certificate using any of the following three methods:

   From the vCenter server:

   a. Copy the file rui.crt from the vCenter server to a location accessible on your Cloud Connectors.
   b. On the Cloud Connector, navigate to the location of the exported certificate and open the rui.crt file.

   Download the certificate using a web browser: If you are using Internet Explorer, depending on your user account, you must right-click on Internet Explorer and choose **Run as Administrator** to download or install the certificate.

   a. Open your web browser and make a secure web connection to the vCenter server (for example `<https://server1.domain1.com>`).
   b. Accept the security warnings.
   c. Click the address bar displaying the certificate error.
   d. Click **Certificate is not valid**, and then click the **Details** tab.
   e. Click **Export..**
   f. Save the exported certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

g. Navigate to the location of the exported certificate and open the .CER file.

Import directly from Internet Explorer running as an administrator:

a. Open your web browser and make a secure web connection to the vCenter server (for example `<https://server1.domain1.com>`).

b. Accept the security warnings.

c. Click the address bar displaying the certificate error.

d. View the certificate.

3. Import the certificate into the certificate store on each Cloud Connector.

a. Click **Install certificate**, select **Local Machine**, and then click **Next**.

b. Select **Place all certificates in the following store**, and then click **Browse**. On a later supported version: Select **Trusted People** and then click **OK**. Click **Next** and then click **Finish**.

IMPORTANT:

If you change the name of the vSphere server after installation, you must generate a new self-signed certificate on that server before importing the new certificate.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For VMware specific information, see Create a VMware catalog.

More information

- Create and manage connections and resources
- VMware virtualization environments.
- VMware cloud and partner solutions

Connection to VMware cloud and partner solutions

After setting up Azure VMware Solution (AVS) cluster, Google Cloud VMware Engine, and VMware cloud on AWS, create the connections. See Connection to VMware virtualization environments for creating connections.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For VMware specific information, see Create a VMware catalog.

More information

- Create and manage connections and resources
- VMware virtualization environments.
- VMware cloud and partner solutions

Connection to XenServer®

Create and manage connections and resources provides detailed instructions using the wizard to create a connection. Before establishing a connection to XenServer (formerly Citrix Hypervisor), you need to first finish setting up your XenServer as a host. See Add a resource type or activate an unused domain in Citrix Cloud.

Create a connection to XenServer

When you create a connection to XenServer, you must provide the credentials for a Virtual Machine Power Administrator (VM Power Admin) or higher-level user.

Citrix recommends using HTTPS to secure communications with XenServer. To use HTTPS, you must replace the default TLS certificate installed on XenServer. For more information, see Install a TLS certificate on your server.

You can configure high availability if it is enabled on the XenServer server. Citrix® recommends that you select all servers in the pool (from **Edit High Availability**) to allow communication with the XenServer server if the pool master fails.

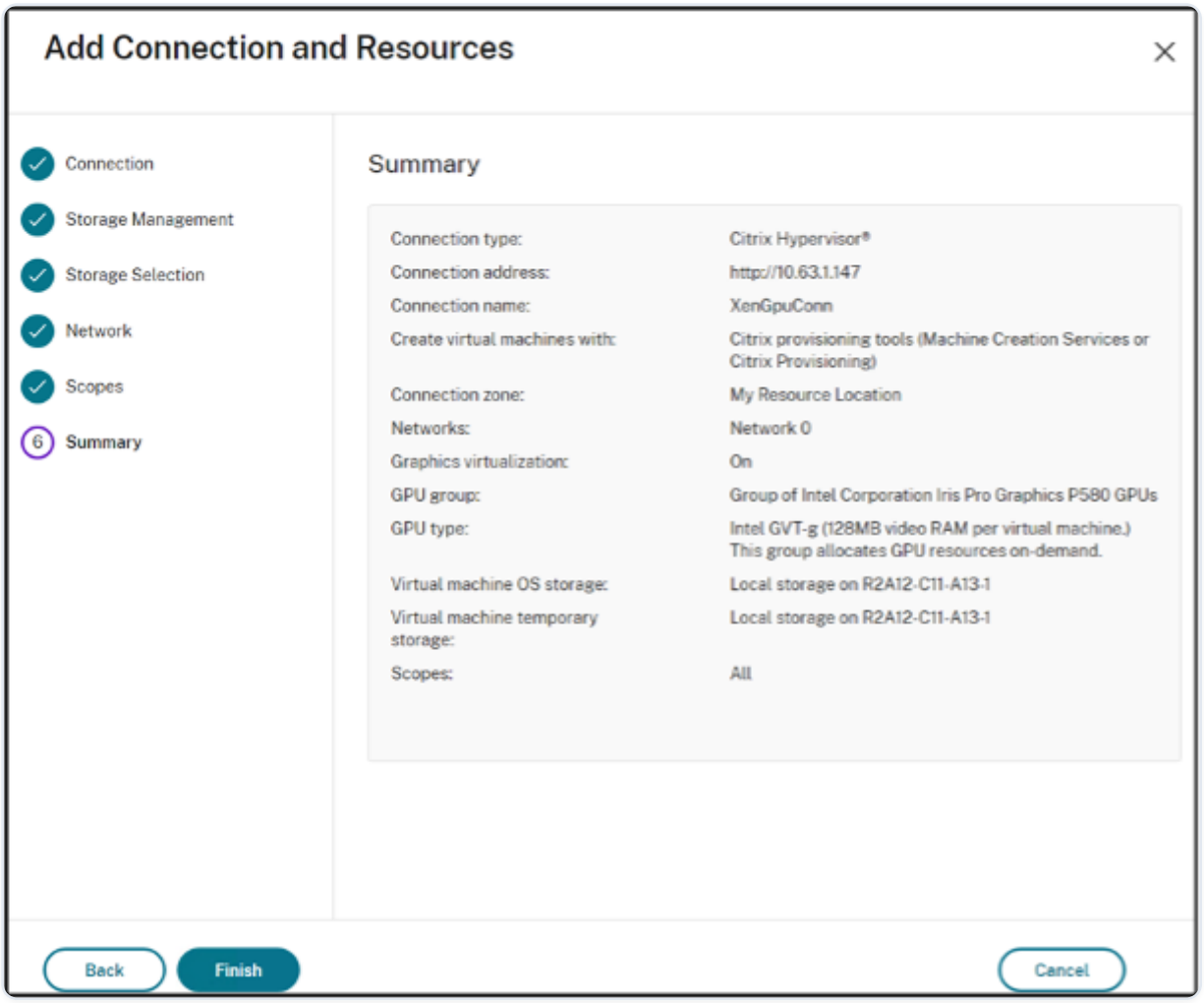
NOTE:

If you are using HTTPS and want to configure high-availability servers, you can now install a wildcard certificate for all servers in a pool.

When using local storage on one or more XenServer hosts for temporary data storage, make sure that each storage location in the pool has a unique name. (To change a name in XenCenter®, right-click the storage and edit the name property.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you connect to the XenServer that supports vGPU, you can verify the GPU group and the GPU type in the **Summary** page of the wizard for creating a connection.



Use IntelliCache™ for XenServer connections

Using IntelliCache, hosted VDI deployments are more cost-effective because you can use a combination of shared storage and local storage. This enhances performance and reduces network traffic. The local storage caches the master image from the shared storage, which reduces the amount of reads on the shared storage. For shared desktops, writes to the differencing disks are written to local storage on the host and not to shared storage.

The important considerations are:

- Shared storage must be NFS when using IntelliCache.
- Citrix recommends that you use a high-performance local storage device to ensure the fastest possible data transfer.

To use IntelliCache, enable IntelliCache as detailed:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When installing XenServer, select **Enable thin provisioning**. See Install the XenServer host for information on installing XenServer host from local media. Citrix does not support mixed pools of servers with some servers that have IntelliCache enabled and some servers that do not IntelliCache enabled.
- In Citrix DaaS™, IntelliCache is disabled by default. You can change the setting only when creating a XenServer connection. You cannot disable IntelliCache later. When you create a XenServer connection:
  - Select **Shared** as the storage type.
  - Select the **Use IntelliCache** checkbox.

See IntelliCache for more information.

Required XenServer permissions

The XenServer permissions are role-based (RBAC). The Role-Based Access Control (RBAC) feature in XenServer allows you to assign users, roles, and permissions to control who has access to your XenServer and what actions they can perform. The XenServer RBAC system maps a user (or a group of users) to defined roles (a named set of permissions). The roles have associated XenServer permissions to perform certain operations.

For more information, see Role-based access control.

The role hierarchy, in order of increasing permissions is: Read-Only → VM Operator → VM Admin → VM Power Admin → Pool Operator → Pool Admin.

The following section summarizes the minimum role required for each provisioning task.

Creating a host connection

TASK	MINIMUM ROLE REQUIRED
Add a host connection using the information obtained from XenServer	Read-Only
View users and their assigned role	Read-Only

Power management of VMs

TASK	MINIMUM ROLE REQUIRED
Power on or off the VMs	VM Operator

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Creating, updating, or deleting VMs

TASK	MINIMUM ROLE REQUIRED
Add or remove VMs to existing snapshots schedules	VM Power Admin
Add, modify, delete snapshot schedules	Pool Operator
Publish master image	Pool Operator (Requires switch-port locking)
Create a machine catalog	Pool Operator: Requires switch-port locking
Add or remove VMs (not GPU enabled VMs)	VM Admin
Add or remove VMs (GPU enabled VMs)	Pool Operator
Add, remove, or configure virtual disk or CD devices	VM Admin
Manage Tags	VM Operator

For more information on RBAC roles and permissions, see RBAC roles and permissions.

For information on switch port locking, see Use switch port locking.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs.
- For XenServer specific information, see Create a XenServer catalog.

More information

- Create and manage connections and resources
- XenServer virtualization environments

Service accounts

A service account is a container for stored credentials, which is configured and used to perform machine identity related operations without user interaction. Create the service account before the operations that require permissions for machine identity management.

You can configure an MCS machine catalog to use a service account to:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- create or delete computer accounts in Active Directory without entering the domain credentials every time.
- manage stale Microsoft Entra joined or Microsoft Intune enrolled devices without manually deleting them through the Microsoft Entra ID or Intune portal.

Supported service account types

Citrix® allows the creation of two types of service accounts based on the type of identity provider.

IDENTITY PROVIDER TYPE	DESCRIPTION	CREDENTIALS
On-premises Active Directory service account	Manages machine catalogs and computer accounts without entering domain credentials every time.	User name and password of an on-premises Active Directory user accounts.
Microsoft Entra service account	Combines a service principal with device management capability to grant permissions for device management.	Application ID and secret of a Microsoft Entra service principal .

Credential protection

Citrix stores the credentials of service accounts in the customer's site database. In DaaS, the site database is a per tenant (customer) database, which is accessible only by the services running for the customer.

The following actions are also enforced to protect the stored credentials:

- The credentials are encrypted using **AES 256** encryption before storing into the database.
- The encryption key is generated per site and stored in the Delivery Controller™ locally, which can only be accessed by the services dedicated to the customer.
- The connection to the database is encrypted using the TLS 1.2 protocol.

On-premises Active Directory service accounts

An on-premises Active Directory service account is a container to store the user name and password of a privileged domain user account. The user account must have sufficient permissions to manage computer accounts in an Active Directory. Machine Creation Service can use this

© 1997–2026 Citrix Systems, Inc. All rights reserved.

service account to do computer accounts related operations without entering the domain credentials every time.

Create an on-premises Active Directory service account

Create an on-premises Active Directory service account using Studio or PowerShell.

Prerequisite

To create an on-premises Active Directory service account, make sure to complete the following task:

- Create a domain user account in your Active Directory with sufficient permissions to create, update, and delete computer objects in your Active Directory or specific OUs.

Use Studio

1. In the **DaaS** tile, click **Manage**.
2. In the left pane, select **Administrators**.
3. In the **Service Accounts** tab, click **Create Service Account**.
4. On the **Identity Type** page, select **On-premises Active Directory**. Click **Next**.
5. On the **Credentials** page, click **Enter credentials** to provide the username and password of a privileged domain user account which you want to use as the service account.
6. Set the password expiration date or leave it as never expired.
7. Select one or more scopes for this service account.
8. Enter a friendly name and a description (optional) for the service account.
9. Click **Finish** to complete the creation.

Use PowerShell

You can use PowerShell commands to create an on-premises Active Directory service. For example:

```
$credential = ConvertTo-SecureString -String $password -AsPlainText -Force

New-AcctServiceAccount -IdentityProviderType ActiveDirectory
-IdentityProviderIdentifier test.local -AccountId test\svcacct_mcs
-AccountSecret $credential -SecretExpiryTime 2030/08/15 -DisplayName
'scvacct_mcs' -Description 'Service account for test.local'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The `$password` is the matching password for the provided domain user account.

Perform machines identity-related actions

After an Active Directory or a Microsoft Entra hybrid based identity pool is associated with a service account, you can do various machines identity-related actions without requiring to enter the domain credentials.

- To create a new identity account using a service account

```
New-AcctADAccount -IdentityPoolName MyPool -Count 2 -UseServiceAccount
```

- To repair the identity accounts using a service account

```
Repair-AcctADAccount -ADAccountName "Domain\account","Domain\account2"
-UseServiceAccount
```

- To remove identity accounts using service account

```
Remove-AcctADAccount -IdentityPoolName MyPool -RemovalOption Delete
-ADAccountName "Domain\account","domain\account2" -UserServiceAccount
```

Where to go next

- To create on-premises Active Directory joined catalogs, see Identity pool of on-premises Active Directory joined machine identity.
- To manage service accounts, see Manage service accounts.

Microsoft Entra service accounts

A Microsoft Entra service account is a container to store application ID and secret of a Microsoft Entra service principal , which has sufficient permissions to manage Microsoft Entra joined or Microsoft Intune enrolled devices. MCS can use this service account to automatically clean any stale Microsoft Entra or Microsoft Intune devices generated during the lifecycle of the provisioned machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Permissions required for a Microsoft Entra service principal

The permissions required for a Microsoft Entra service principal used by a service account depend on the capabilities enabled for the service account.

- For the service account with Microsoft Entra joined devices management capability, the Microsoft Entra service principal must have `Device.ReadWrite.All` permission in your Microsoft Entra tenant.
- For the service account with Microsoft Intune enrolled devices management capability, the Microsoft Entra service principal must have `DeviceManagementManagedDevices.ReadWrite.All` permission in your Microsoft Entra tenant.
- For the service account with Microsoft Entra security group management capability, the Microsoft Entra service principal must have `Group.ReadWrite.All` and `GroupMember.ReadWrite.All` permissions in your Microsoft Entra tenant.

Limitation

Microsoft Entra role-based access control is currently not supported. Therefore, assign the Microsoft Entra permissions directly to the service principal.

Create a Microsoft Entra service account

Use Studio or PowerShell to create a Microsoft Entra service account.

Prerequisite

To create a Microsoft Entra service account, make sure to complete the following task:

- Create a Microsoft Entra principal in your Microsoft Entra tenant with sufficient permissions based on the capabilities that you want to enable the service account with.

Use Studio

1. In the **DaaS** tile, click **Manage**.
2. In the left pane, select **Administrators**.
3. In the **Service Accounts** tab, click **Create Service Account**.
4. On the **Identity Type** page, select **Microsoft Entra ID**. A new option to route the traffic is enabled.
    a. Select the **Route traffic through Citrix Cloud Connectors** checkbox.
    b. Select the zones available to route the traffic and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. On the **Credentials** page, enter the Microsoft Entra tenant ID, Application ID, and Client secret and set the credential expiration date.
6. Choose the capabilities for the service account.
7. Select one or more scopes for the service account.
8. Enter a friendly name and a description (optional) for the service account.
9. Click **Finish** to complete the creation.

NOTE:

- The capability of Microsoft Entra joined devices management is selected by default and you cannot deselect it.
- To use a multitenant Microsoft Entra application, which is invited to your tenant, the Microsoft Entra tenant ID you entered must be your own tenant ID rather than the home tenant ID of the application.

Use PowerShell

Alternatively, you can use PowerShell commands to create a Microsoft Entra service account. For example:

```
$tenantId = xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

$applicationId = xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

$applicationSecret = xxxxxxxxxxxxxxx

$credential = ConvertTo-SecureString -String $applicationSecret
-AsPlainText -Force



New-AcctServiceAccount -IdentityProviderType AzureAD
-IdentityProviderIdentifier $tenantId -AccountId $applicationId
-AccountSecret $credential -SecretExpiryTime 2030/08/15 -Capabilities
@("AzureADDeviceManagement","IntuneDeviceManagement") -DisplayName
'MyApplication' -Description 'Service account for Microsoft Entra tenant'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrate Microsoft Entra joined device management to service account

Previously, Citrix® provided an option to enable Microsoft Entra joined device management when creating or editing a hosting connection to Microsoft Azure Resource Manager. MCS used the permissions of the Microsoft Entra service principal (provisioning SPN) stored along with the hosting connection to manage the stale Microsoft Entra joined device. With service accounts, you can use a dedicated Microsoft Entra service principal (identity management SPN) stored along with a service account to manage Microsoft Entra joined or Microsoft Intune enrolled devices.

Citrix recommends migrating from hosting connection-powered device management to service account-powered device management to separate the responsibility of provisioning SPN and identity management SPN.

For any existing hosting connections that are already enabled with Microsoft Entra joined device management, you can disable it as follows:

1. From Studio, select **Hosting** in the left pane.
2. Select the connection and then select **Edit Connection** in the action bar.
3. On the **Connection Properties** page, clear the **Enable Microsoft Entra joined device management** checkbox.
4. Click **Save** to apply the changes.

NOTE:

Currently, you cannot enable Microsoft Entra joined device management when creating a new hosting connection.

Route Microsoft Entra device management and security group management traffic

Create and modify a Microsoft Entra service account to route Microsoft Entra device management and security group management traffic from Delivery Controller to Microsoft Entra ID through Citrix Cloud Connector.

Include the following custom property while creating or modifying a Microsoft Entra service account:

```
CustomProperties: {"ProxyHypervisorTrafficThroughConnector":true,"ZoneUid":["<zone uid>"]}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The `$ZoneUid` is the Uid of the zone (resource location) that the network traffic wants to be routed to. Obtain the Uid from `Get-ConfigZone` command.

For example:

- For creating a new Microsoft Entra service account:

```
$tenantId = xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

$applicationId = xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

$applicationSecret = xxxxxxxxxxxxxxx

$SecureString = ConvertTo-SecureString -String "Secretstring"
-AsPlainText -Force

New-AcctServiceAccount -IdentityProviderType AzureAD
-IdentityProviderIdentifier "<Identity provider ID>" -AccountId
"<Account ID>" -AccountSecret $SecureString -SecretExpiryTime <yyyy-mm-
dd>  -Capabilities
@("AzureADDeviceManagement","IntuneDeviceManagement") -DisplayName
"<Display name>" -CustomProperties
'{"ProxyHypervisorTrafficThroughConnector":true,"ZoneUid":["<Zone
UID>"]}'
```

- For modifying an existing Microsoft Entra service account:

```
Set-AcctServiceAccount -ServiceAccountUid $serviceAccountUid
-CustomProperties
'{"ProxyHypervisorTrafficThroughConnector":true,"ZoneUid":[$ZoneUid]}'
```

Where to go next

- To create Microsoft Entra joined catalogs, see Identity pool of Microsoft Entra joined machine identity.
- To manage service accounts, see Manage service accounts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage service accounts

Managing service accounts is a critical aspect to ensure that they remain in a healthy state and their credentials are up-to-date. This article describes the steps to view, rename, edit, test, and delete a service account.

View service account details

1. In the **DaaS** tile, click **Manage**.
2. In the left pane, select **Administrators**.
3. Select the **Service Accounts** tab.
4. Select a service account and view its details in the lower panel. See the properties of each service account along with its associated machine catalogs and troubleshooting tips in the lower panel.

Error or warning icons appear beside a service account if:

- the service account is in an unhealthy state.
- the credential of a service account is nearing expiry.

The **Troubleshooting** tab provides information to diagnose and fix the issues.

NOTE:

After fixing the issues, do a service account test to refresh the status. For more information, see Test a service account.

Rename a service

1. In the **DaaS** tile, click **Manage**.
2. In the left pane, select **Administrators**.
3. Select the **Service Accounts** tab.
4. Select a service account and click **Rename**.

Edit a service account

1. In the **DaaS** tile, click **Manage**.
2. In the left pane, select **Administrators**.
3. Select the **Service Accounts** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select a service account and click **Edit**.

Test a service account

1. In the **DaaS** tile, click **Manage**.
2. In the left pane, select **Administrators**.
3. Select the **Service Accounts** tab.
4. Select a service account and click **Test Service Account**.

- For an on-premises Active Directory service account, credentials are verified during testing.
- For Microsoft Entra service account, application ID and secret along with the required permissions are verified during testing.

Identity and fix the issues according to the recommendations. The **Troubleshooting** tab provides information to diagnose and fix the issues. After fixing the issues, test the service account.

Delete a service account

Before deleting a service account, make sure that the service account is not used by any MCS machine catalogs.

1. In the **DaaS** tile, click **Manage**.
2. In the left pane, select **Administrators**.
3. Select the **Service Accounts** tab.
4. Select a service account and click **Delete**.

Image management

Introduction

The MCS catalog creation or update process has two phases:

- Mastering: a source image is converted into a published image
- Cloning: new VMs are created from the published image

With the image management functionality, MCS separates the mastering phase from the overall provisioning workflow.

You can prepare various MCS image versions (Prepared Image) from a single source image and use it across multiple different MCS machine catalogs. You can also share prepared image

© 1997–2026 Citrix Systems, Inc. All rights reserved.

versions across hosting units. This implementation significantly reduces the storage and time costs, and simplifies the VM deployment and image update process.

The benefits of using this image management functionality are:

- Generate prepared images in advance without creating a catalog.
- Reuse prepared images in multiple scenarios, such as creating and updating a catalog.
- Significantly reduce catalog creation or update time.
- Share prepared image versions across hosting units:
  - For Azure, Nutanix AHV Prism Central, and VMware, image versions can be shared across host connections of the same connection type.
  - For Amazon WorkSpaces Core Managed Instances, image versions can be shared across different availability zones, tied to different hosting units, within the same AWS region or in different regions.
  - For AWS EC2, image versions can be shared across different availability zones, tied to different hosting units, within the same AWS region.
  - For XenServer, image versions can only be shared across hosting units within the same host connection.

NOTE:

- This feature is currently applicable to Amazon WorkSpaces Core Managed Instances, AWS EC2, Azure, Nutanix AHV Prism Central, Red Hat OpenShift, VMware virtualization, and XenServer environments.
- You can create an MCS machine catalog without using prepared images. In that case, you cannot get the benefits of the feature. However, for Amazon WorkSpaces Core Managed Instances, create the MCS catalog using only a prepared image version. You can’t create the catalog using a master image directly.

Use cases

Some of the use cases of image management functionality are:

- *Version management*: Image versions allow you to:
  - manage different iterations or updates to a particular image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - maintain multiple versions of an image for different purposes.

- *Logical grouping*: You can create multiple image definitions to:
    - logically group image versions based on various criteria such as project, department, or application and desktop type.
    - manage images more efficiently within an organization.
- *Image sharing*: You can share prepared image versions across hosting units within host connections of the same connection type to:
    - ensure consistency and uniformity of images across different hosting units.

What is a prepared image?

With the image management functionality, MCS decouples the mastering phase from the overall catalog creation or update workflow and breaks down the process into two stages:

1. Create prepared images from a single source image.
2. Use the prepared image to create or update an MCS machine catalog.

You can create the prepared images in advance. You can use a single prepared image to create or update multiple MCS provisioned machine catalogs.

Understand how a prepared image is used across multiple MCS machine catalogs when you use Studio:

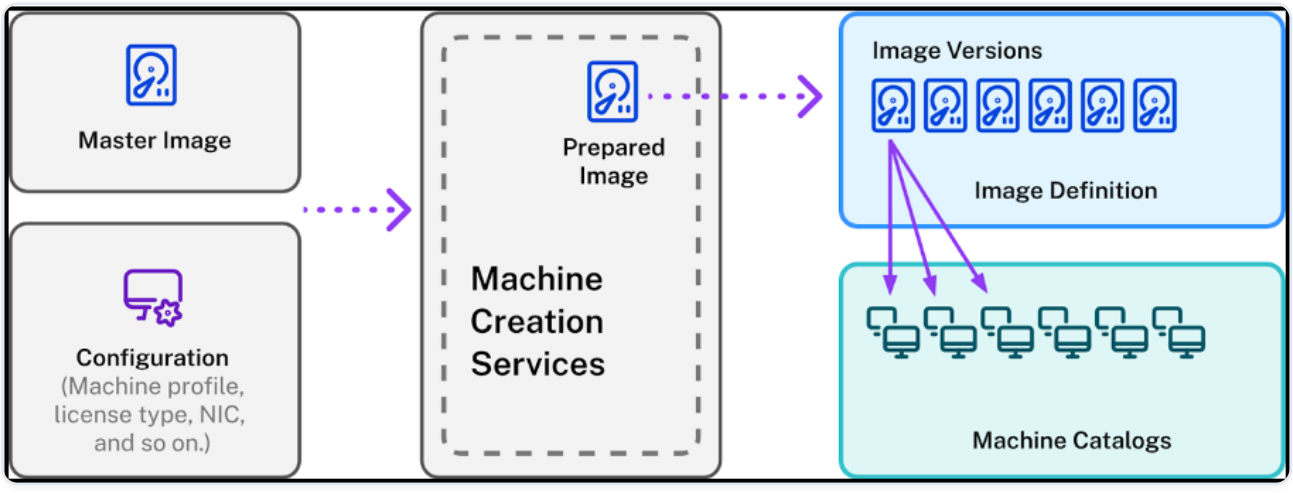


Image definition: Image definitions are a logical grouping of versions of an image. The image definition holds information about:

- why the image was created
- what OS it is for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- other information about using the image.

A catalog isn't created from an image definition, but from the image versions that are created based on the image definition.

Image version: Image versions manage versionings for the image definition. An image definition can have multiple image versions. Use the image versions as prepared images to create or update a catalog.

- For Azure and VMware, image versions can be shared across host connections of the same connection type.
- For Amazon WorkSpaces Core Managed Instances, image versions can be shared across different availability zones, tied to different hosting units, within the same AWS region or in different regions.
- For AWS EC2, image versions can be shared across different availability zones, tied to different hosting units, within the same AWS region.
- For XenServer, image versions can only be shared across hosting units within the same host connection.

Alternatively, if you want to use PowerShell commands to create a provisioning scheme to create or update a catalog, then you must create a prepared image version spec based on the master image version spec as needed for your environment.

- For Azure, Nutanix AHV Prism Central, and VMware, image versions can be shared across host connections of the same connection type.
- For Amazon WorkSpaces Core Managed Instances, image versions can be shared across different availability zones, tied to different hosting units, within the same AWS region or in different regions.
- For AWS EC2, image versions can be shared across different availability zones, tied to different hosting units, within the same AWS region.
- For XenServer, image versions can only be shared across hosting units within the same host connection.

Requirement

- For Windows master images, only VDA images version 2311 or later are supported. The MCS/IO component must be explicitly selected and installed. Enabling or disabling the MCS I/O configuration must be determined during machine catalog creation or updates, as it is not enabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations

Currently, the feature does not support the following:

- Multiple NIC in Azure
- Persistent data disk feature
- Hibernation for multi-session
- Image type change
- While sharing prepared image version across hosting unit in Azure, the following sharing methods are not allowed:
  - Share Directly
  - Share to public community gallery

Image lifecycle management using Studio

Lifecycle of the image when you use Studio is as follows:

1. Create a prepared image: Create an image definition and its initial image version.
2. Create image versions from the initial image version.
3. If needed, share an image version with a hosting unit in your virtualization environment.
4. Use an image version as a prepared image to create catalogs.
5. Update a machine catalog with a different prepared image.
6. Manage the image definitions and versions: Edit the name and description of image versions, and description of an image definition.
7. Delete an image version.
8. Delete an image definition.

Alternatively, you can also manage images using PowerShell. See Image lifecycle management using PowerShell.

Image lifecycle management using PowerShell

If you want to use PowerShell commands to create a provisioning scheme, then you must create a prepared image version spec based on the master image version spec as needed for your environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Master image version spec: A master image version spec is a specific image added or created under an image version. You can add an existing image in the hypervisor as a master image version spec or create a prepared image version spec based on the master image version spec as needed for your environment. The prepared image version spec can be used for multiple provisioning schemes.

You can share image version specs across hosting units, depending on your virtualization environment:

- In Azure, VMware, and Amazon WorkSpaces Core Managed Instances environments, you can share image version specs across hosting units, whether they are in the same or different host connections of the same connection type. In Azure, the sharing is achieved using the disk sharing capability of Azure Compute Gallery (ACG).
- For AWS EC2, image versions can be shared across different availability zones, tied to different hosting units, within the same AWS region.
- In Nutanix AHV Prism Central and XenServer, you can share image version specs only across hosting units within the same host connection.

Lifecycle of an image when using PowerShell commands is:

1. Create an image:
    a. Create an image definition.
    b. Add a new configuration for Image Definition in specified hosting connection.
    c. Create an image version.
    d. Add a master image version spec.
    e. Create a prepared image version spec.
2. If needed, share an image version spec with another hosting unit, following the sharing constraints of your virtualization environment:
    - For Azure and VMware, image versions can be shared across host connections of the same connection type.
    - For Amazon WorkSpaces Core Managed Instances, image versions can be shared across different availability zones, tied to different hosting units, within the same AWS region or in different regions.
    - For AWS EC2, image versions can be shared across different availability zones, tied to different hosting units, within the same AWS region.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For XenServer, image versions can only be shared across hosting units within the same host connection.

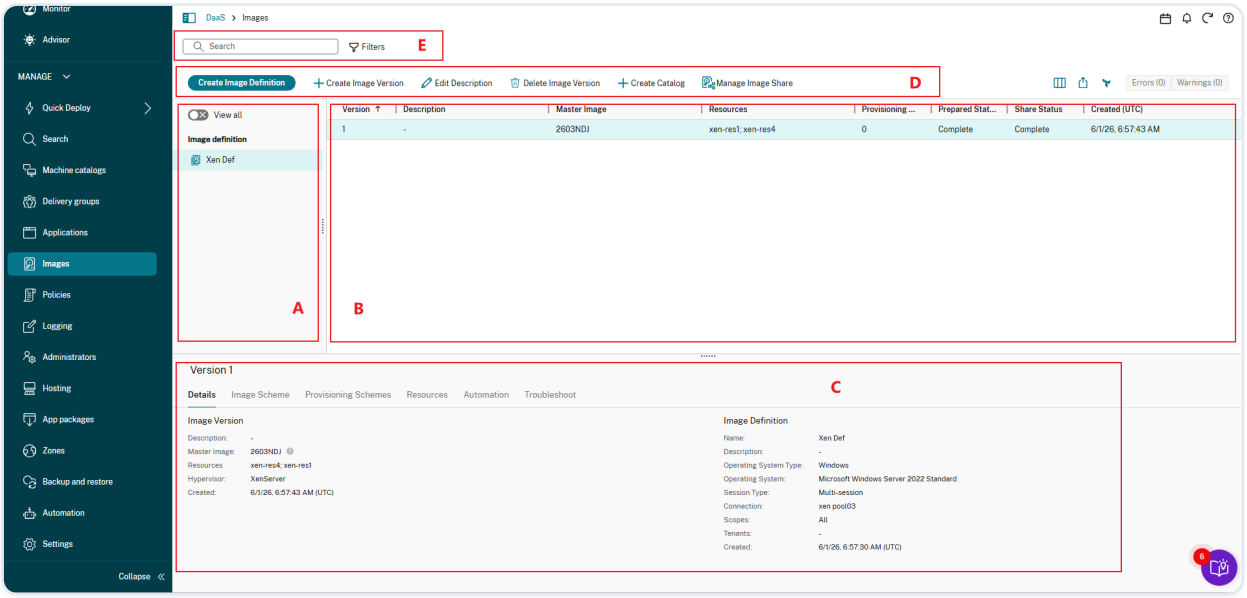
3. Create an MCS machine catalog using a prepared image version spec:
    a. Create a broker catalog.
    b. Create an identity pool.
    c. Create a provisioning scheme with the parameter of prepared image version spec Uid using the `New-ProvScheme` command.
    d. Link the broker catalog with the provisioning scheme.
4. Create VMs in the MCS machine catalog.
5. Change the prepared image version spec of a provisioning scheme using `Set-ProvScheme` command.
6. Manage the image definitions and versions: Edit the image versions and image definitions.
7. Delete an MCS machine catalog: The deletion order is: machine catalog > shared prepared image version spec (if image sharing) > prepared image version spec > master image version spec > image version > configuration for image definition in the specified hosting connection > image definition. Before deleting the image version spec, ensure that the prepared image version spec is not associated with any MCS machine catalog.

Understand Images node

Use the **Images** node to create and manage MCS-prepared images. Its main view is divided into four parts:

- With prepared image being shared across host unit: In Azure and VMware

© 1997–2026 Citrix Systems, Inc. All rights reserved.



LABEL	PART	DESCRIPTION
A	Image definitions	Lists the previously created image definitions.
B	Image versions	Displays image versions for the selected image definition. When **View all** is turned off, only the selected image definition's versions are displayed. When it is turned on, image versions across all definitions are displayed.
C	Details	• The **Details** tab displays detailed information about the selected image definition or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PART	DESCRIPTION
		version such as Master Image, Resource, Hypervisor, name of the image definition, OS type, and session type. • The **Image Scheme** tab displays information about the template used for preparing images such as hard disk, machine size, license type, disk encryption set, machine profile, and so on. • The **Provisioning Schemes** tab displays the provisioning scheme name used for creating the catalog. • The **Troubleshoot**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PART	DESCRIPTION
		tab provides the error status of the selected image version. • In case of image sharing: The **Resources** tab provides the status of image version share.
D	Action bar	Lists the actions that you can take on image definitions and versions such as **Create Image Version**, **Edit Description**, **Manage Image Share**(in case of prepared image sharing), **Delete Image Version**, and **Create Catalog**.
E	Search bar	Specifies filter criteria for searching image versions that meet the conditions.

Create prepared image machine catalogs

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Studio
- PowerShell commands

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Currently, you can create prepared image machine catalogs in Amazon WorkSpaces Core Managed Instances, AWS EC2, Azure, Red Hat OpenShift, VMware, and XenServer® virtualization environments.

NOTE:

You can create an MCS machine catalog without using prepared images. In that case, you cannot get the benefits of the feature. However, for Amazon WorkSpaces Core Managed Instances, create the MCS catalog using only a prepared image version. You can't create the catalog using a master image directly.

Where to go next

- Create catalogs using prepared images in Amazon WorkSpaces Core Managed Instances
- Create catalogs using prepared images in AWS EC2
- Create catalogs using prepared images in Azure
- Create catalogs using prepared images in Red Hat OpenShift
- Create catalogs using prepared images in VMware
- Create catalogs using prepared images in XenServer

Create catalogs using prepared images in Amazon WorkSpaces Core Managed Instances

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Studio
- PowerShell

Key steps

1. Create the image definition and the initial image version.
2. Create image versions from the initial image version.
3. Use the image version as a prepared image to create a catalog.

Create an image definition and initial image version using Studio

To create an image definition and the initial image version, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. From Studio, go to the **Images** node, and click **Create Image Definition**. Click **Next** on the **Introduction** page.
2. On the **Image Definition** page, specify the **OS type** and **Session type** for the image definition.
3. On the **Image** page, select **Resources** (only the resources applicable for the set connection are listed), a master image to use as a template for creating the image version, and a machine profile for capturing hardware properties from. Select a machine profile to capture hardware properties from a VM instance or launch template version.

   NOTE:

   - Before selecting an image, verify that the master image has VDA 2311 or later installed and the MCSIO driver is installed on the VDA.
   - The Instance Metadata Service (IMDS) V2 is only supported and not IMDS V1. For information, see How Instance Metadata Service Version 2 works.

4. On the **Machine Specification** page, select a machine size. The machine size of the machine profile (selected on the **Image** page) is selected by default.
5. On the **NICs** page, select or add NICs for the preparation image. For each NIC, select an associated VPC subnet.
6. On the **Version Description** page, enter a description for the initial image version created.
7. On the **Summary** page, verify the details of the image definition and the initial image version created. Enter a name and description for the image definition. Click **Finish**.

Create image versions using Studio

Image versions allow for the management of different iterations or updates to a particular image. This functionality enables you to maintain multiple versions of an image for different purposes.

To create image versions from the initial image version, do the following:

NOTE:

The hosting unit of all the image versions must be the same.

1. Go to the **Images** node, select an image version or an image definition, and click **Create Image Version**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the **Image definition** page, you can change the hosting unit, and reselect the master image and machine profile for that image version.
3. If you want the configuration of the image version to be different from the initial configured image version, then configure the settings on the **Machine Specification** and **NICs** pages of the **Create Image Version** dialog.
4. Add a description for the image version. Click **Finish**.

NOTE:

If the creation of the image version fails for any reason, the **Troubleshoot** tab at the bottom provides a **Retry** option.

Create a prepared image version spec using PowerShell

The detailed PowerShell commands to create a prepared image version spec are as follows:

1. Check the available image definition names using the `Test-ProvImageDefinitionNameAvailable command`. For example,

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. Create an image definition using the `New-ProvImageDefinition` command. For example,

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

3. Create a new configuration for image definition in the specified Hosting connection using the `Add-ProvImageDefinitionConnection` command.

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName test-conn
```

4. Create an image version using the `New-ProvImageVersion` command. For example,

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Add a master image version spec to the image version using the `Add-ProvImageVersionSpec` command. For example,

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName wsc -MasterImagePath "XDHyp:
\HostingUnits\wsc\win10-2411-ami (ami-00123456789abcdef).template”"
```

> **NOTE:**
>
> You can add only one master image version spec to one image version for a hosting unit.

6. Create a prepared image version spec from the master image version spec using the `New-ProvImageVersionSpec` command. The `SourceImageVersionSpecUid` parameter is derived from the `Add-ProvImageVersionSpec` command. For example,

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  00000000-0000-0000-0000-00000000000

-MachineProfile 'XDHyp:\HostingUnits\wsc\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -RunAsynchronously
```

Example of the complete set of PowerShell commands to create image definition, image version, and prepared image version spec:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession




Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName wsc -CustomProperties $CustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\wsc\win10-2411-ami
(ami-00123456789abcdef).template”



New-ProvImageVersionSpec -MachineProfile 'XDHyp:
\HostingUnits\wsc\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
00000000-0000-0000-0000-00000000000-HostingUnitName wsc

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

NOTE:

- All image version specs in an image definition must belong to the same hosting unit.
- An image version can have only one master image version spec and one prepared image version spec.
- All image version specs must have a machine profile.

Share prepared images across availability zones and regions

You can now share a single prepared image across different availability zones, tied to different hosting units, within the same AWS region or in different regions for your Amazon WorkSpaces Core Managed Instances. This lets you use one prepared image to create and update MCS machine catalogs in various availability zones and regions. When sharing across different AZs in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

different regions, the prepared image version will be copied from the original region to the destination regions.

You can maintain a single prepared image and use it to create and update machine catalogs across multiple availability zones and regions tied to different hosting units. This significantly reduces your image management overhead, ensures consistency across deployments, and streamlines the provisioning process. You can also seamlessly update existing machine catalogs with prepared images from a different availability zone or region.

Use cases

- **Centralized Image Management:** You create a prepared image in one availability zone (for example, `us-east-1a`). You can then share this image to other availability zones like `us-east-1b` within the same `us-east-1` AWS region or `us-west-1a` in a different `us-west-1 region`. This allows a single image to serve multiple hosting units and simplifies maintenance for you.
- **Efficient Catalog Creation and Updates:** You can use a prepared image created in `AZ 1` (for example, `us-east-1a`) to create new catalogs in `AZ 1`. After sharing this image to `AZ 2` (for example, `us-east-1b`), you can then use the shared image in `AZ 2` to create and update catalogs in `AZ 2`.
- **Cross-hosting unit and hosting connection deployments:** If your environment has multiple hosting units under the same or different AWS regions, you can efficiently share prepared images between these hosting units.

Limitations

- **Sharing within same AWS Account**: You cannot share across different AWS Accounts in the current implementation.

Important considerations

- **Deletion order:** To delete an original prepared image version specification, you must first delete all its shared image version specifications. Alternatively, you must delete the original and shared specifications simultaneously.
- **Image Version dependency:** When you remove an image version, you must first remove any sharing configurations that depend on that specific image version. Catalogs that you created from the original (unshared) image can remain intact.
- **Catalog back-portability:** You can update existing machine catalogs that you deployed before this feature's introduction. Use prepared images that you created in a different availability zone or region from where you originally deployed the catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Complete deletion:** When you delete a prepared image, you can no longer use it in any availability zone where you shared or originally created it. Moreover, a prepared image version cannot be deleted until all catalog tied the prepared image version are deleted first.

Prerequisites

Before you configure or use this feature, ensure that you meet the following conditions:

- Your environment must be an Amazon WorkSpaces Core Managed Instances environment.
- You must configure multiple hosting units (each can be tied to different availability zones) and host connections (each can be tied to a different region) under the same AWS account.

Configure using Studio UI

You can share prepared images across availability zones tied to different hosting units using the Studio UI.

TO SHARE A PREPARED IMAGE

1. Navigate to the **Images** node of the Studio and select the prepared image version you wwant to share with other availability zones.
2. Select **Manage Image Share** at the top navigation bar to manage the image sharing for the selected image version.
3. On the **Manage Image Share** page, select one or more resources you want to share the image version with. The resources can be in different availability zones from that of the original image version.
4. Click **Save** to share the image version in the resources across other availability zones. The image version is updated such that it is shared across the different resources that you selected. Once complete, use the image version to create catalogs in the availability zones the image version is shared across.

TO REMOVE SHARING OF A PREPARED IMAGE

1. On the **Images** node of the Studio, select the prepared image version you would like to remove from sharing.
2. Select **Manage Image Share** at the top navigation bar to manage the image sharing for the selected image version.
3. Clear the checkboxes from one or more resources (availability zones) that you want to stop sharing the image version with.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> The resources must no longer have any catalogs associated with and created from the shared image version. Any catalogs created from the shared image version to be removed must be deleted first.

4. Click **Save** to remove sharing of the resources across the cleared availability zones. The image version is updated such that it is no longer shared in those availability zones.

Configure using PowerShell

Alternatively, you can share prepared images across availability zones tied to different hosting units using PowerShell commands.

TO SHARE A PREPARED IMAGE

1. Ensure that you have the `ImageVersionSpecUid` of the prepared image you want to share. You can retrieve this using `Get-ProvImageVersionSpec` or similar `Get-` commands in PowerShell.
2. Determine the `HostingUnitName` of the availability zone (can be the same or a different region) where you want to make the prepared image available. This is the name of the hosting unit you configured for that specific AZ.
3. **Run the `Add-ProvImageVersionSpecHostingUnit` command:** Use the following PowerShell command. Replace `<ImageVersionSpecUid>` with your image's Uid and `<targetHostingUnitName>` with the name of the hosting unit in the target availability zone that you want to share the image version specification to:

   ```
   Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
   <ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
   ```

4. After successful execution, you can see the image's status in the Studio UI indicating that you shared it with the specified hosting unit.

TO REMOVE SHARING OF A PREPARED IMAGE

1. Ensure you have the `ImageVersionSpecUid` of the prepared image from which you want to remove sharing.
2. Determine the `HostingUnitName` of the availability zone from which you want to remove the shared image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Run the `Remove-ProvImageVersionSpecHostingUnit` command:** Use the following PowerShell command. Replace `<ImageVersionSpecUid>` with your image's Uid and `<targetHostingUnitName>` with the name of the hosting unit in the target Availability Zone that you want to remove the sharing of the image version specification from:

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

Network setting during image preparation

During image preparation, a preparation virtual machine (VM) is created based on the original VM. This preparation VM is disconnected from the network. To disconnect the network from the preparation VM, a network security group is created to deny all inbound and outbound traffic. This network security group persists and is reused. The network security group's name is `Citrix.XenDesktop.IsolationGroup-GUID`, where GUID is randomly generated.

A machine profile-based machine catalog

You can use a machine profile to capture the hardware properties from an EC2 instance (VM) or launch template version and apply them to the provisioned machines. Properties that are captured can include, for example, tenancy type, instance type, security groups, network mappings, EBS volume properties, EBS optimization, CPU options, hibernation capability, and other supported AWS configurations.

You can use an AWS EC2 Instance (VM) or AWS Launch Template version as the machine profile input.

NOTE:

- EBS volume properties are derived only from a machine profile.
- The Instance Metadata Service (IMDS) V2 is only supported and not IMDS V1. For information, see How Instance Metadata Service Version 2 works.

AWS tenancy

AWS provides the following tenancy options: shared tenancy (the default type) and dedicated tenancy. Shared tenancy means that multiple Amazon WorkSpaces Core instances from different customers might reside on the same piece of physical hardware. Dedicated tenancy means that

© 1997–2026 Citrix Systems, Inc. All rights reserved.

your Amazon WorkSpaces Core instances run only on hardware with other instances that you have deployed.

NOTE:

The dedicated instances are only supported (dedicated hosts are currently not supported). Other customers do not use the same piece of hardware.

Tenancy type is captured from machine profile

When you use MCS to create a catalog to provision machines in AWS, the tenancy type is captured from the machine profile.

- **Shared hardware**: This setting is suitable for most deployments. Multiple customers share pieces of hardware even though they do not interact with each other. Using shared hardware is the least expensive option for running your Amazon EC2 instances.
- **Dedicated instance**: This setting is more suitable for deployments with specific security or compliance requirements. With a dedicated instance, you still enjoy the benefits of having a host separate from other AWS customers but you do not pay for the entire host. You do not need to worry about the capacity of the host but you are charged at a higher rate for the instances. Additionally, Dedicated Instances provide limited support for Bring Your Own License (BYOL).

Flexible billing

Amazon WorkSpaces Core Managed Instances supports two billing modes:

BILLING MODE	DESCRIPTION
Monthly	Fixed, monthly flat-rate billing. Ideal for persistent desktops and predictable workloads.
Hourly	Pay-as-you-go billing. This is the AWS default configuration if no billing mode is explicitly specified.

These options provide flexibility for managing compute costs based on your workload's persistence and usage patterns.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature requires the use of the Amazon WorkSpaces billing service. By default, MCS uses this service to provision and manage instances, letting you benefit from more competitive flat-rate pricing for persistent workloads.

Prerequisites and considerations

- AWS account configuration: Your AWS account must be configured to use the WorkSpaces billing service. While AWS accounts are switched by default, some customers may request AWS to remain on the legacy EC2 billing service for using WorkSpaces Core Managed Instances.

  NOTE:

  If your account is on the legacy EC2 billing service, the **Monthly** billing option is not available.

- Host connection: Flexible billing is only applicable to Amazon WorkSpaces Core host connections. It is not supported for standard AWS EC2 host connections.
- Spot instances: Spot instances are not supported with the WorkSpaces billing service.
- Mixed billing: An AWS account must use either WorkSpaces billing or EC2 billing for core managed instances. A mix of both within a single account is not supported.
- Compatibility: Only specific instance types, platform types (OS), and tenancy types are compatible with certain billing modes. MCS performs a preflight check to ensure your selections (Service Offering, Machine Profile, and Prepared Image) match the chosen billing mode.

See Create a machine catalog with a specific billing mode.

Create a catalog

A prepared image and a machine profile is required for creating catalogs of Amazon WorkSpaces Core Managed Instances. You can use an AWS VM Instance or AWS Launch Template version as the machine profile input.

NOTE:

Currently, creation of catalogs of both persistent and non-persistent VMs (`CleanOnBoot` property is `True` or `False`) is supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Before creating a catalog of Amazon WorkSpaces Core Managed Instances, you need to finish creating:

1. A connection to Amazon WorkSpaces Core Managed Instances. See Connection to Amazon WorkSpaces Core Managed Instances
2. A prepared image.

You can create a catalog using:

- Studio
- PowerShell

Create a catalog using Studio

Create a machine catalog from the Images node

Use the **Create catalog** option in the **Images** node to create a catalog using the image version.

Alternatively, you can select the version when creating a catalog in the **Machine Catalogs** node, linking to the prepared image option in the catalog creation workflow. See Create a machine catalog from the Machine Catalogs node.

To create an MCS machine catalog from the **Images** node, do the following:

1. Select an image version and click **Create catalog**. Click **Next** on the **Introduction** page.
2. On the **Machine Management** and **Image** pages, the settings are pre-selected based on the selected image version. On the Image page, enter a note for the selected prepared image.
3. Complete the settings on the following pages.
4. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.
5. Go to the **Machine Catalogs** node to see the created machine catalog.

Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the Machine Catalogs node, do the following:

1. Click **Machine Catalogs** on the left navigation pane.
2. Click **Create Machine Catalog**. The **Machine Catalog Setup** page appears.
3. On the **Machine Type** page, select a machine type for the catalog, for example, **Multi-session OS**.
4. On the **Machine Management** page, select the following settings:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Select **Machines that are power managed (for example, virtual machines or blade PCs)**.

b. Select **Citrix provisioning technology**. Then, select **Citrix Machine Creation Services™**.

c. In the **Resources** field, select the resources (Availability Zone or Local Zone) that you configured while creating the host connection and click **Next**.

5. On the **Desktop experience** page, select either random or static desktop that you want users to have when they log in. If a static desktop is selected, further specify whether you want to save changes that the user makes on the local disk (persistent or non-persistent).
6. On the **Image** page, click **Select an image** to select a prepared image for the machine catalog. Select the prepared version that you created. Click the image version name. To view more details about the selected image version, click the version number, which is underlined. Click **Done**.

   The machine profile associated with the prepared image appears and its hardware properties (for example, instance type, tenancy type, network mappings, security groups, volume properties) are used to create machines in the catalogs. To change the machine profile source to another VM or launch template version click the edit button.
7. On the **Virtual Machines** page:

   a. Enter the number of VMs for the catalog.

   b. The default machine specification is displayed, which is based on the machine profile. To change it, select the edit icon and select a machine specification.
8. On the **NICs** page, select the NICs (or ENIs) for the VMs.
9. On the **Machine Identities** page, configure the machine identity type for the machines in the catalog:

   a. To configure **domain-joined machines (on-premises Active Directory or Microsoft Entra hybrid joined)**, select the domain and create new AD accounts for the VMs to be created in this machine catalog. The provisioned VMs are joined to the domain selected. To provision **non-domain joined machines**, select the non-domain join option.

   b. Specify the account naming scheme for the new accounts to be created for the VMs.
10. On the **Domain credentials** page, click **Enter credentials** to provide the credentials for the selected domain. Enter admin-level username and password when prompted. You can also use

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a service account if you have domain credentials already saved previously by following our product docs.

11. Click through the remaining pages until the **Summary** page. Enter a name for the machine catalog and select **Finish** to create the machine catalog.

Limitations on creating a machine catalog in an AWS local zone

- Certain local zones only support certain hardware configurations (for example, Perth local zone does not support GP3 volumes, only GP2).
- Since only gp2 is universally supported across all local zones, and not all support gp3, ID disk creation defaults to using gp2 volume type.
- You must select a machine profile with hardware specifications that are supported in the desired local zone.
- Prepared image AMIs snapshots and ID disk snapshots defaults to being placed in the region, rather than the local zone (due to AWS limitations regarding visibility into EBS snapshot support in local zones).
- Only local zones supporting full EC2 and EBS services are supported zones.

Create a catalog using PowerShell

Create a catalog using a prepared image version spec and machine profile

- Create an MCS non-persistent machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$true] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

- Create an MCS persistent machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$false] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

Example of the complete set of Powershell commands to create a catalog:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "wsccatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "domainname"
-IdentityPoolName "wsccatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "aws##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName wsccatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName wsc -IdentityPoolName wsccatalog -CleanOnBoot -Scope @()
-SecurityGroup @() -MachineProfile 'XdHyp:\HostingUnits\cvad-test-
scalestress\us-east-1a.availabilityzone\machine-profile-instance i
(i-0xxxxxxx).vm' -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName wsccatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Update the machine profile

To update the machine profile on a catalog that was initially provisioned with a machine profile, do the following. You can also change the tenancy type and hibernation capability of the machine profile source while editing an MCS machine catalog.

1. Run `Set-ProvScheme` command. For example,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

Create a machine catalog with a specific billing mode

You can specify the billing mode while creating a machine catalog using only PowerShell currently.

To specify the billing mode through PowerShell, use the `CustomProperties` parameter in the `New-ProvScheme` command.

```
$custprop = "BillingMode,Monthly"



New-ProvScheme -ProvisioningSchemeName "MyCatalog" `

-ImageVersionSpecUid $ImageVersionSpecUid `

-HostingUnitName "wsc-unit" `

-IdentityPoolName "MyIdentityPool" `

-MachineProfile "XdHyp:\HostingUnits\wsc-unit\machine-profile
lt-123.launchtemplate\lt-123 (1).launchtemplateversion" `

-CustomProperties $custprop `

-CleanOnBoot
```

NOTE:

If the `BillingMode` property is omitted, the catalog defaults to `Hourly`.

CHANGE THE BILLING MODE OF AN EXISTING CATALOG

You can convert an existing catalog from `Monthly` to `Hourly`, or vice versa. This change can apply to both new and existing VMs in the catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT CONSIDERATIONS FOR UPDATES

- Service window: Existing VMs must undergo a service window or power cycle to apply the billing change.
- Validation: MCS validates that the existing instance types and platforms are compatible with the new billing mode before applying the change.

UPDATE USING POWERSHELL

- To update the billing mode of only new VMs added to a catalog, update the billing mode custom property of the provisioning scheme:

```
$custprop = "BillingMode,Hourly"



Set-ProvScheme -ProvisioningSchemeName "MyCatalog" -CustomProperties
$custprop
```

- To update the billing mode of new and existing VMs in a catalog, create a new provisioning scheme version with the updated custom property, and apply the new version to all VMs:

```
$custprop = "BillingMode,Hourly"



New-ProvSchemeVersion -ProvisioningSchemeName "MyCatalog"
-CustomProperties $custprop



New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 2 `

-StartsNow -AllVMs `

-MaxDurationInMinutes 100 `

-ProvisioningSchemeName "MyCatalog"
```

MONITOR BILLING INFORMATION

You can verify the billing mode for catalogs and individual virtual machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Run the following PowerShell commands to check your account's billing eligibility:

- Returns `BillingMode` as part of CustomProperties

```
Get-ProvScheme –ProvisioningSchemeName “"MyCatalog" "  | Select
 ProvisioningSchemeName,  CustomProperties
```

- Returns `BillingMode` as part of VMInfo

```
Get-ProvVMDetails –ProvisioningSchemeName “"MyCatalog" "  | Select-
Object  -ExpandProperty VMInfo
```

TROUBLESHOOTING AND VALIDATION

MCS includes preflight checks to prevent incompatible configurations. You may encounter the following errors during catalog creation or editing:

- **NoInstanceConfigFoundForBillingMode**: Occurs if the selected Service Offering (instance type), Tenancy, and Platform Type are not supported for the chosen billing mode.
- **Spot Instance Not Supported**: If you attempt to use Spot instances with a WorkSpaces host connection, validation fails.
- **EC2 billing restriction**: If your AWS account is on the legacy EC2 billing model, attempting to set a Monthly billing mode results in a validation error.

Create a catalog with launch template version using PowerShell

You can create an MCS machine catalog with a launch template version as a machine profile input. You can also update the input of a machine profile catalog from a VM to a launch template version and from a launch template version to a VM.

On the AWS EC2 console, you can provide the instance configuration information of a launch template along with version number. When you specify the launch template version as a machine profile input while creating or updating a machine catalog, the properties from that version of the launch template are copied to the provisioned VDA VMs.

The following properties can be provided using machine profile input or explicitly as parameters in `New-ProvScheme` or `Set-ProvScheme`commands. If they are provided in `New-ProvScheme` or `Set-ProvScheme` commands, they take precedence over the machine profile values of these properties.

- Service Offering

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Networks

NOTE:

If service offering is not provided in the machine profile launch template or as a parameter in the `New-ProvScheme` command, you get an appropriate error.

To create a catalog using launch template version as a machine profile input:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Get the list of launch template versions of a launch template. For example:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. Create an identity pool if not created. For example:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. Create a provisioning scheme with a launch template version as a machine profile input. For example:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-ImageVersionSpecUid ‘24dfb047-e867-527g-896c-25664xxxxx1t’ `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. Register a provisioning scheme as a broker catalog. For example:

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. Complete creating the catalog.

Update the machine profile source

You can also update the input of a machine profile catalog from a VM to a launch template version and from a launch template version to a VM. For example:

- To update the input of a machine profile catalog from a VM to a launch template version:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx
(1).launchtemplateversion"
```

- To update the input of a machine profile catalog from a launch template version to a VM:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

MCSIO enabled catalog

MCS Storage Optimization (MCSIO) improves virtual machine I/O performance by caching disk write operations through a two-tier mechanism:

- in memory, or
- on a dedicated high-speed disk (overflows to disk when memory is full).

For Amazon WorkSpaces Core Managed Instances, enabling MCSIO attaches a Write-Back Cache (WBC) disk to each provisioned VM in addition to the standard OS and Identity disks.

Enable and configure MCSIO using:

- Studio
- PowerShell

Use Studio to enable MCSIO

PREREQUISITES

Before configuring MCSIO in Studio, ensure the following:

- The MCSIO driver is installed on the master image (AMI). When installing or upgrading the VDA, select the option to install the MCSIO driver. By default, the driver is not installed.
- A prepared image version is created from a master image that includes the MCSIO driver.
- The machine catalog uses a non-persistent (CleanOnBoot) desktop experience. MCSIO applies to non-persistent VDI catalogs.

CREATE AN MCSIO-ENABLED MACHINE CATALOG USING STUDIO

Complete the preceding catalog creation steps (Machine Type, Machine Management, Desktop Experience, Image, Virtual Machines, NICs, Machine Identities, Domain Credentials) as described in Create a catalog. When you reach the Disk Settings page, do the following:

1. On the **Disk Settings** page, select the **Enable and configure write-back cache for optimum I/O performance** checkbox.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Configure the write-back cache disk settings:

   - **Disk cache size (GB)**: Enter the size in gigabytes of the disk used for caching. The value must be at least 1 GB and must not exceed the OS disk size.
   - **Disk drive letter**: Select Auto-assigned to let the system assign a drive letter, or specify a drive letter manually.
   - **Memory allocated to cache (MB)**: Enter the amount of memory in megabytes to allocate for caching. The value must be greater than zero and less than the total machine memory.

   NOTE:

   Write-back cache requires that the MCSIO driver is installed on the master image.

3. Under **Select the storage type for the write-back cache disk**, select an EBS SSD volume type:

   Storage Type:

   - General Purpose SSD (gp2)
   - General Purpose SSD (gp3)
   - Provisioned IOPS SSD (io1)
   - Provisioned IOPS SSD (io2)

   NOTE:

   Write-back caching supports EBS SSD volume types only. HDD volume types and local instance storage (ephemeral storage) are not supported.

4. Under **Select the persistence type for the write-back cache disk**, select one of the following:

   - **Use non-persistent write-back cache disk**: The cache disk is created when the machine powers on and deleted when it powers off. This is the default.
   - **Use persistent write-back cache disk**: The cache disk is retained across power cycles.

5. Under **System disk**, optionally select **Retain system disk during power cycles** to keep the OS disk when the machine powers off. When enabled, machines skip recreating the root disk from the template on each boot, which reduces boot time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For optimal boot performance, enable both **Use persistent write-back cache disk** and **Retain system disk during power cycles**. With both options enabled, machines reuse the existing cache disk and OS disk on startup rather than initializing new ones.

6. Click **Next** to proceed through the remaining wizard pages.
7. On the **Summary** page, verify the MCSIO-related settings before finishing. The summary displays the following write-back cache fields:
   - Enable temporary disk cache
   - Memory cache size (MB)
   - Disk cache size (GB)
   - Persistent with write-back cache disk
   - Write-back cache disk type
   - Write-back cache disk drive letter
   - Retain system disk
8. Enter a name and optional description for the machine catalog, then click **Finish**.

UPDATE MCSIO SETTINGS ON AN EXISTING CATALOG USING STUDIO

You can update write-back cache settings on an existing catalog from **Edit Machine Catalog**.

NOTE:

Changes you make on the **Disk Settings** page apply only to new machines you add to the catalog later. Existing machines remain unchanged.

1. From **Machine Catalogs**, select the catalog to update and click **Edit Machine Catalog**.
2. Navigate to the **Disk Settings** page. Update any of the following settings:
   - **Disk cache size (GB)**: Change the size of the write-back cache disk.
   - **Memory allocated to cache (MB)**: Change the memory allocated for caching.
   - **Storage type**: Change the EBS volume type for the write-back cache disk.
   - **Persistence type**: Toggle between persistent and non-persistent write-back cache disk.
   - **Retain system disk during power cycles**: Enable or disable OS disk retention.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click **Apply** to save without closing, or **Save** to save and close.

EBS DISK LAYOUT FOR MCSIO-ENABLED MACHINES

When MCSIO is enabled, each provisioned Amazon WorkSpaces Core VM has three EBS volumes attached. You can verify the disk layout from the AWS Management Console under the Elastic Block Store section of the EC2 instance details.

DISK	DEVICE INDEX	DESCRIPTION
OS disk	/dev/sda1	Root volume cloned from the prepared image. If Retain system disk during power cycles is enabled, this disk persists when the machine powers off.
Identity disk	xvdf	Stores machine identity information for the provisioned VM. Always persists.
Write-back cache disk	xvdg	High-speed cache disk for MCSIO write operations. Persists across power cycles only if Use persistent write-back cache disk is selected.

WRITE-BACK CACHE AND OS DISK BEHAVIOR REFERENCE

The following table summarizes how write-back cache and OS disk behave based on the persistence settings selected.

WBC PERSISTENCE	OS DISK RETENTION	ON POWER-OFF	BOOT PERFORMANCE	STORAGE COSTS WHEN VM POWERED-OFF
Non-persistent (default)	Disabled (default)	Both WBC disk and OS disk are deleted. New disks are created on next power-on.	Standard	No OS disk or WBC disk costs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WBC PERSISTENCE	OS DISK RETENTION	ON POWER-OFF	BOOT PERFORMANCE	STORAGE COSTS WHEN VM POWERED-OFF
Non-persistent (default)	Enabled	WBC disk is deleted. OS disk is retained.	Faster — skips OS disk initialization	OS disk costs, no WBC disk costs.
Persistent	Disabled (default)	WBC disk is retained. OS disk is deleted and recreated from template on next power-on.	Faster — skips WBC initialization	WBC disk costs, no OS disk costs.
Persistent	Enabled	Both WBC disk and OS disk are retained.	Fastest — no disk initialization required	OS disk and WBC disk costs.

NOTE:

Enabling OS disk retention on a non-persistent catalog means the OS disk is not reset on reboot. This trades faster boot times for storage costs of the OS disk. All writes, though, still only go to the Write-back memory cache or Write-back cache disk. User changes are not accumulated on the OS disk even when enabling OS disk retention. Evaluate based on your environment requirements.

USE POWERSHELL TO ENABLE MCSIO

CREATE AN MCSIO ENABLED CATALOG USING POWERSHELL

The four parameters added to the New-ProvScheme PowerShell command are:

- `UseWriteBackCache`: Turns on caching (write-back cache) for the given provisioning scheme
- `WriteBackCacheDiskSize`: Specifies the size in GB of the temporary disk used for caching
- `WriteBackCacheMemorySize`: Specifies how much memory in MB to use for caching. This is an optional parameter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- The value of `WriteBackCacheDiskSize` must be more than zero because at least 1 GB of cache disk storage is required. The cache disk size must not be bigger than the OS disk size.
- The value of `WriteBackCacheMemorySize` must be non-zero and less than the machine catalog memory size.

The custom properties that affect MCSIO are:

- `WBCDiskStorageType`: Defines the volume type, which is used for the temporary disk in Amazon WorkSpaces Core Managed Instances. This parameter takes a string argument in the format `volume-type[:iops][:throughput]`. The following are the volume types:
  - gp2: Do not use iops and throughput parameters for this volume type
  - gp3: Use iops and throughput parameters for this volume type
  - io1: Use only iops parameter for this volume type
  - io2: Use only iops parameter for this volume type

  The default volume type is **gp2**.
- `PersistWBC`: Controls whether to keep or discard the cache disk whenever the Amazon WorkSpaces Core Managed Instances is powered off. If set to `true`, the cache disk is kept. If set to `false` (the default), the cache disk is only created and kept while the AMI instance is powered on.
- `PersistOSDisk`: Controls whether to keep or discard the OS disk whenever the Amazon WorkSpaces Core Managed Instances is powered off. If set to `true`, the OS disk is kept. If set to `false` (the default), the OS disk is only created and kept while the AMI instance is powered on.

Perform the following steps in the PowerShell window to create an MCSIO enabled non-persistent catalog:

1. Open the PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create a broker catalog and an identity pool.
4. Create the provisioning scheme. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'



$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. Add VMs to the catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improve boot performance with MCSIO

You can improve the boot performance of VMs if you enable MCSIO and set `PersistWBC` and `PersistOSDisk` custom properties as `true`. With such a setting, VMs can boot faster because they do not need to initialize a new cache disk or to recreate a root disk from their template.

Encrypt OS and ID disks

You can create a catalog of VMs with AWS KMS keys (Customer managed key and AWS managed key) that can be used to encrypt OS disk and Identity Disk (ID).

- AWS managed keys are automatically rotated every year.
- Customer managed keys are optional for automatic rotation and can be managed manually.

You can see the following AWS documents for more information on KMS keys:

- AWS KMS concepts
- How automatic key rotation works

For encryption of OS and ID disks, configure one of the following:

- Use a prepared image that is encrypted (for example, an AMI created from an instance or snapshot that contains an EBS root volume encrypted with KMS key)
- Use a machine profile source (VM or launch template) that contains an encrypted EBS root volume.

Limitations

Consider the following limitations:

- MCS currently supports only one disk on prepared image AMI.
- You cannot directly encrypt existing unencrypted EBS volumes or snapshots, or modify the KMS key of an existing encrypted volume. To do that, you must:

  a. Create a new snapshot of that volume.

  b. Create a new volume from that snapshot

  c. Encrypt the new volume.

See the following AWS documents:

- Encrypt unencrypted resources
- Limitations of automatic or default encryption of EBS volumes: Automatically encrypt existing and new Amazon EBS volumes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a catalog with disk encryption

You can create an MCS machine catalog with disk encryption using:

- Prepared image (created using image management from master image that has encrypted disk)
- Machine profile

Considerations while using machine profile input are:

- The KMS key of the machine profile input takes precedence over the prepared image's KMS key.
- If no machine profile input is provided, then the KMS key of the prepared image AMI is used to encrypt the disks of catalog VMs.
- If the machine profile has Block Device Mappings present, then the block devices present in the prepared image template (AMI) and the machine profile must match. For example, if AMI has a device defined on `/dev/sda1`, then the Machine Profile must also have a device defined on `/dev/sda1`.
- If there is no key in the machine profile source and the prepared image is unencrypted, then disks of catalog VMs are not encrypted.
- When the prepared image is encrypted, a machine profile source VM or launch template must have an encrypted root volume to be considered a valid input.

Modify an existing catalog

You can modify an existing catalog using the `Set-ProvScheme` PowerShell command to have:

- A machine profile input with a volume containing a new KMS key.
- A prepared image created from the master image with encrypted AMI using image management.

Important considerations:

- The volumes of new VMs added to the catalog are encrypted with the new KMS key.
- To update the encryption settings when there is an existing machine profile, run `Set-ProvScheme` with a new machine profile.
- You cannot modify an existing catalog from having encrypted volumes to unencrypted volumes. You cannot do an image update from an encrypted prepared image AMI to an unencrypted prepared image AMI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable NitroTPM and UEFI secure boot for VM instances

When creating a catalog, you can now select a prepared image (AMI) with NitroTPM and/or UEFI secure boot enabled. Accordingly, the provisioned VMs in the catalog are also enabled with NitroTPM and/or UEFI secure boot. This implementation ensures that the VMs are secured and trusted. For more information on NitroTPM and UEFI Secure Boot, see the Amazon documentation.

Limitations

- You can use both NitroTPM and Secure Boot currently in all AWS Regions (including the AWS GovCloud (US) Regions) except China.
- You cannot enable NitroTPM and UEFI secure boot on existing catalogs. If you want a catalog with NitroTPM and UEFI secure boot enabled, create a new catalog.

Key steps

1. Set up your AWS environment.
2. Create a connection to AWS.
3. Create a master image (AMI) enabled with NitroTPM and/or UEFI secure boot.
4. Create a prepared image from the master image. See Create a prepared image for Amazon WorkSpaces Core Managed Instances.
5. Create a machine catalog by selecting the prepared image with NitroTPM and UEFI secure boot enabled in Citrix Studio catalog creation menu or when creating a Provisioning Scheme using PowerShell commands.

VMs added to the created catalog have NitoTPM and UEFI secure boot enabled.

Create an AMI that supports NitroTPM and UEFI secure boot

1. You can create an AMI from a VM that has NitroTPM and/or UEFI secure boot enabled.
    a. Create the instance from using the AWS marketplace images. Example, search for `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`.
    b. Download single or multi session VDA.
    c. Create an AMI from that VM.
2. Use the register-image command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
--boot-mode (string)

--tpm-support (string)
```

For more information, see register-image.

See the following AWS documents:

- Determine the supported boot modes of an EC2 instance type
- Requirements for using NitroTPM with Amazon EC2 instances/.

You can open a PowerShell window from the Delivery controller™ host to check if a specific:

- service offering supports NitroTPM or UEFI secure boot

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- template supports NitroTPM or UEFI secure boot

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

Update the service offering of existing catalog

You can change the service offering of an existing catalog using `Set-ProvScheme`. The change applies to the newly added VMs. However, you get errors in the following scenarios:

AMIS BOOT MODE	AMI SUPPORTS NITRO TPM?	SERVICE OFFERING SUPPORTS NITROTPM AND UEFI SECURE BOOT?
UEFI	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AMIS BOOT MODE	AMI SUPPORTS NITRO TPM?	SERVICE OFFERING SUPPORTS NITROTPM AND UEFI SECURE BOOT?
Legacy BIOS	Yes	No
UEFI	Yes	No
UEFI Preferred	Yes	No

Copy tags on VMs

You can copy tags on NICs, and disks (Identity disk, write back cache disk, and OS disk) that are specified in the machine profile to newly created VMs in an MCS machine catalog. You can specify these tags in any of the machine profile sources (AWS VM instance or AWS launch template version). This feature is applicable to persistent and non-persistent machine catalogs and VMs.

NOTE:

- On the AWS EC2 console, you cannot see the **Tag Network Interfaces** values under the **Launch Template Version Resource Tags**. However, you can run the PowerShell command `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` to see the tag specifications.
- If a machine profile source (VM or launch template version) has two network interfaces (eni-1 and eni-2), and eni-1 has tag t1 and eni-2 has tag t2, then the VM gets both the two network interfaces' tags.

Filter VM instances using PowerShell

An AWS VM instance that you use as a machine profile VM must be compatible for the machine catalog to create and function correctly. To list the AWS VM instances that can be used as machine profile input VMs, you can use the `Get-HypInventoryItem` command. The command can page and filter the inventory of VMs available on a hosting unit.

Pagination:

Get-HypInventoryItem supports two modes of pagination:

- Paging mode uses the `-MaxRecords` and `-Skip` parameters to return sets of items:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - `-MaxRecords`: The default is **1**. This controls how many items to return.
  - `-Skip`: The default is **0**. This controls how many items to skip from the absolute beginning (or absolute end) of the list in the hypervisor.

- Scrolling mode uses `-MaxRecords`, `-ForwardDirection`, and `-ContinuationToken` parameters to allow scrolling of the records:
  - `-ForwardDirection`: The default is **True**. This is used along with `-MaxRecords` to return either the next set of matching records or the previous set of matching records.
  - `-ContinuationToken`: The returns the items immediately after (or before if `ForwardDirection` is **false**) but not including the item given in the `ContinuationToken`.

Examples of pagination:

- To return a single record of the machine template with the lowest name. The `AdditionalData` field has the `TotalItemsCount` and the `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- To return 10 records of the machine template with the lowest name:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- To return an array of records ending with the highest name:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- To return an array of records starting at the machine template associated with the given `ContinuationToken`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filtering:

The following additional optional parameters are supported for filtering. You can combine these parameters with the pagination options.

- `-ContainsName "my_name"`: If the given string matches part of an AMI name, then the AMI is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: If an AMI has at least one of these tags, it is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

NOTE:

Two tag values are supported. **Not Tagged** tag value matches items which do not have the given tag in their list of tags. **All values** tag value matches items which have the tag regardless of the value of the tag. Otherwise, the match happens only if the item has the tag and the value equals to what is given in the filter.

- `-Id "ami-0a2d913927e0352f3"`: If the AMI matches the given ID, it is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxxx
```

Filtering on AdditionalData parameter:

The `AdditionalData` filter parameter lists templates or VMs based on their capability, service offering, or any property which is in AdditionalData. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

You can also add a `-Warn` parameter to indicate the incompatible VMs. The VMs are included with an `AdditionalData` field named **Warning**. For example:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

Where to go next

- Manage catalogs created using prepared images

More information

- Image management
- For Amazon WorkSpaces Core GitHub PowerShell examples, see citrix-mcs-sdk-samples-Amazon WorkSpaces Core

Create catalogs using prepared images in AWS EC2

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Studio
- PowerShell commands

The key steps to create an MCS machine catalog using the prepared image are:

1. Create the image definition and the initial image versions.
2. Use the image version as a prepared image to create a catalog

Create an image definition and initial image version

Use Studio

To create an image definition and the initial image version, do the following:

1. From Studio, go to the **Images** node, and click **Create Image Definition**. Click **Next** on the **Introduction** page.
2. On the **Image Definition** page, specify the **OS type** and **Session type** for the image definition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Image** page, select **Resources** (only the resources applicable for the set connection are listed), a master image to use as a template for creating the image version, and a machine profile for capturing hardware properties from. Select a machine profile to capture hardware properties from a VM instance or launch template version.

   NOTE:

   - Before selecting an image, verify that the master image has VDA 2311 or later installed and the MCSIO driver is installed on the VDA.
   - The Instance Metadata Service (IMDS) V1 and V2 are both supported.

4. On the **Machine Specification** page, select a machine size. The machine size of the machine profile (selected on the **Image** page) is selected by default.
5. On the **NICs** page, select or add NICs for the preparation image. For each NIC, select an associated VPC subnet.
6. On the **Version Description** page, enter a description for the initial image version created.
7. On the **Summary** page, check the details of the image definition and the initial image version created. Enter a name and description for the image definition. Click **Finish**.

CREATE IMAGE VERSIONS

Image versions allow for the management of different iterations or updates to a particular image. This functionality enables you to maintain multiple versions of an image for different purposes.

To create image versions from the initial image version, do the following:

NOTE:

The hosting unit of all the image versions must be the same.

1. Go to the **Images** node, select an image version or an image definition, and click **Create Image Version**.
2. On the **Image definition** page, you can change the hosting unit, and reselect the master image and machine profile for that image version.
3. If you want the configuration of the image version to be different from the initial configured image version, then configure the settings on the **Machine Specification** and **NICs** pages of the **Create Image Version** dialog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Add a description for the image version. Click **Finish**.

> **NOTE:**
>
> If the creation of the image version fails for any reason, the **Troubleshoot** tab at the bottom provides a **Retry** option.

Use PowerShell

The detailed PowerShell commands to create a prepared image version spec are as follows:

1. Check the available image definition names using the `Test-ProvImageDefinitionNameAvailable command`. For example,

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. Create an image definition using the `New-ProvImageDefinition` command. For example,

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

3. Create a new configuration for image definition in the specified Hosting connection using the `Add-ProvImageDefinitionConnection` command.

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName test-conn
```

4. Create an image version using the `New-ProvImageVersion` command. For example,

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. Add a master image version spec to the image version using the `Add-ProvImageVersionSpec` command. For example,

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName aws -MasterImagePath "XDHyp:
\HostingUnits\aws\win10-2411-ami (ami-00123456789abcdef).template”"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You can add only one master image version spec to one image version for a hosting unit.

6. Create a prepared image version spec from the master image version spec using the `New-ProvImageVersionSpec` command. The `SourceImageVersionSpecUid` parameter is derived from the `Add-ProvImageVersionSpec` command. For example,

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  00000000-0000-0000-0000-00000000000

-MachineProfile 'XDHyp:\HostingUnits\aws\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -RunAsynchronously
```

Example of the complete set of Powershell commands to create image definition, image version, and prepared image version spec:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession




Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName aws-CustomProperties $CustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    -MasterImagePath "XDHyp:\HostingUnits\aws\win10-2411-ami
(ami-00123456789abcdef).template”



New-ProvImageVersionSpec -MachineProfile 'XDHyp:
\HostingUnits\aws\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
00000000-0000-0000-0000-00000000000-HostingUnitName aws

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

NOTE:

- All image version specs in an image definition must belong to the same hosting unit.
- An image version can have only one master image version spec and one prepared image version spec.
- All image version specs must have a machine profile.

Share prepared images across availability zones and regions

You can now share a single prepared image across different availability zones, tied to different hosting units, within the same AWS region or in different regions for your AWS EC2 environments. This lets you use one prepared image to create and update MCS machine catalogs in various availability zones and regions. When sharing across different AZs in different regions, the prepared image version will be copied from the original region to the destination regions.

You can maintain a single prepared image and use it to create and update machine catalogs across multiple availability zones and regions tied to different hosting units. This significantly reduces your image management overhead, ensures consistency across deployments, and streamlines the provisioning process. You can also seamlessly update existing machine catalogs with prepared images from a different availability zone or region.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use cases

- **Centralized Image Management:** You create a prepared image in one availability zone (for example, `us-east-1a`). You can then share this image to other availability zones like `us-east-1b` within the same `us-east-1` AWS region or `us-west-1a` in a different `us-west-1` region. This allows a single image to serve multiple hosting units and simplifies maintenance for you.
- **Efficient Catalog Creation and Updates:** You can use a prepared image created in `AZ 1` (for example, `us-east-1a`) to create new catalogs in `AZ 1`. After sharing this image to `AZ 2` (for example, `us-east-1b`), you can then use the shared image in `AZ 2` to create and update catalogs in `AZ 2`.
- **Cross-hosting unit and hosting connection deployments:** If your environment has multiple hosting units under the same or different AWS regions, you can efficiently share prepared images between these hosting units.

Limitations

Sharing within same AWS account: In the current implementation, you can share only within the same AWS account.

Important considerations

- **Deletion order:** To delete an original prepared image version specification, you must first delete all its shared image version specifications. Alternatively, you must delete the original and shared specifications simultaneously.
- **Image Version dependency:** When you remove an image version, you must first remove any sharing configurations that depend on that specific image version. Catalogs that you created from the original (unshared) image can remain intact.
- **Catalog back-portability:** You can update existing machine catalogs that you deployed before this feature's introduction. Use prepared images that you created in a different availability zone or region from where you originally deployed the catalog.
- **Complete deletion:** When you delete a prepared image, you can no longer use it in any availability zone where you shared or originally created it. Moreover, a prepared image version cannot be deleted until all catalog tied the prepared image version are deleted first.

Prerequisites

Before you configure or use this feature, ensure that you meet the following conditions:

- Your environment must be an AWS EC2 environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You must configure multiple hosting units (each can be tied to different availability zones) and host connections (each can be tied to a different region) under the same AWS account.

Configure using PowerShell

You can share prepared images across availability zones tied to different hosting units using only PowerShell commands currently.

TO SHARE A PREPARED IMAGE

1. Ensure that you have the `ImageVersionSpecUid` of the prepared image you want to share. You can retrieve this using `Get-ProvImageVersionSpec` or similar `Get-` commands in PowerShell.
2. Determine the `HostingUnitName` of the availability zone (can be the same or a different region) where you want to make the prepared image available. This is the name of the hosting unit you configured for that specific availability zone.
3. **Run the `Add-ProvImageVersionSpecHostingUnit` command:** Use the following PowerShell command. Replace `<ImageVersionSpecUid>` with your image's Uid and `<targetHostingUnitName>` with the name of the hosting unit in the target availability zone that you want to share the image version specification to:

   ```
   Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
   <ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
   ```

4. After successful execution, you can see the image's status in the Studio UI indicating that you shared it with the specified hosting unit.

TO REMOVE SHARING OF A PREPARED IMAGE

1. Ensure you have the `ImageVersionSpecUid` of the prepared image from which you want to remove sharing.
2. Determine the `HostingUnitName` of the availability zone from which you want to remove the shared image.
3. **Run the `Remove-ProvImageVersionSpecHostingUnit` command:** Use the following PowerShell command. Replace `<ImageVersionSpecUid>` with your image's Uid and `<targetHostingUnitName>` with the name of the hosting unit in the target availability zone that you want to remove the sharing of the image version specification from:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

Create a machine catalog

Use Studio

CREATE A MACHINE CATALOG FROM THE IMAGES NODE

Use the **Create catalog** option in the **Images** node to create a catalog using the image version.

Alternatively, you can select the version when creating a catalog in the **Machine Catalogs** node, linking to the prepared image option in the catalog creation workflow. See Create a machine catalog from the Machine Catalogs node.

To create an MCS machine catalog from the **Images** node, do the following:

1. Select an image version and click **Create catalog**. Click **Next** on the **Introduction** page.
2. On the **Machine Management** and **Image** pages, the settings are pre-selected based on the selected image version. On the Image page, enter a note for the selected prepared image.
3. Complete the settings on the following pages.
4. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.
5. Go to the **Machine Catalogs** node to see the created machine catalog.

Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the Machine Catalogs node, do the following:

1. Click **Machine Catalogs** on the left navigation pane.
2. Click **Create Machine Catalog**. The **Machine Catalog Setup** page appears.
3. On the **Machine Type** page, select a machine type for the catalog, for example, **Multi-session OS**.
4. On the **Machine Management** page, select the following settings:
    a. Select **Machines that are power managed (for example, virtual machines or blade PCs)**.
    b. Select **Citrix provisioning technology**. Then, select **Citrix Machine Creation Services™**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. In the **Resources** field, select the resources (Availability Zone) that you configured while creating the host connection and click **Next**.

5. On the **Desktop experience** page, select either random or static desktop that you want users to have when they log in. If a static desktop is selected, further specify whether you want to save changes that the user makes on the local disk (persistent or non-persistent).
6. On the **Image** page, click **Select an image** to select a prepared image for the machine catalog. Select the prepared version that you created. Click the image version name. To view more details about the selected image version, click the version number, which is underlined. Click **Done**.

   The machine profile associated with the prepared image appears and its hardware properties (for example, instance type, tenancy type, network mappings, security groups, volume properties) are used to create machines in the catalogs. To change the machine profile source to another VM or launch template version click the edit button.
7. On the **Virtual Machines** page:

   a. Enter the number of VMs for the catalog.

   b. The default machine specification is displayed, which is based on the machine profile. To change it, select the edit icon and select a machine specification.
8. On the **NICs** page, select the NICs (or ENIs) for the VMs.
9. On the **Machine Identities** page, configure on-premises Active Directory or Microsoft Entra hybrid joined for the machines in the catalog by selecting the domain and creating new AD accounts for the VMs to be created in this machine catalog. The provisioned VMs are joined to the domain selected. Specify the account naming scheme for the new AD accounts to be created for the VMs. Click **Next**.
10. On the **Domain credentials** page, click **Enter credentials** to provide the credentials for the selected domain. Enter admin-level username and password when prompted. You can also use a service account if you have domain credentials already saved previously by following our product docs.
11. Click through the remaining pages until the **Summary** page. Enter a name for the machine catalog and select **Finish** to create the machine catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use PowerShell

CREATE A CATALOG USING A PREPARED IMAGE VERSION SPEC AND MACHINE PROFILE

- Create an MCS non-persistent machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$true] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

- Create an MCS persistent machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$false] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

Example of the complete set of Powershell commands to create a catalog:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "awscatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "domainname"
-IdentityPoolName "awscatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "aws##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName awscatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName aws -IdentityPoolName awscatalog -CleanOnBoot -Scope @()
-SecurityGroup @() -MachineProfile 'XdHyp:\HostingUnits\cvad-test-
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
scalestress\us-east-1a.availabilityzone\machine-profile-instance i
(i-0xxxxxxxx).vm' -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName awscatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Where to go next

- Manage catalogs created using prepared images

More information

- Image management

Create catalogs using prepared images in Azure

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Studio
- PowerShell commands

The key steps to create an MCS machine catalog using the prepared image are:

1. Create the image definition and the initial image versions.
2. Use the image version as a prepared image to create a catalog

Use Studio

Create an image definition and initial image version

To create an image definition and the initial image version, do the following:

1. From Studio, go to the **Images** node, and click **Create Image Definition**. Click **Next** on the **Introduction** page.
2. On the **Image Definition** page, specify the **OS type** and **Session type** for the image definition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select an existing resource group or create a new one for holding the image resources. To enable image sharing, select **Store image versions in Azure Compute Gallery** and then choose to create a new gallery or use an existing one to hold its image versions.
4. On the **Image** page, select **Resources** (only the resources applicable for the set connection are listed) and a master image to use as a template for creating the image version. You can select the **Use a machine profile** checkbox and select a machine profile.

   NOTE:

   - Before selecting an image, verify that the master image has VDA 2311 or later installed and the MCSIO driver is installed on the VDA.
   - If you want to use a confidential VM type prepared image to create an MCS catalog, then create a prepared image using the confidential VM type master image and a confidential VM type machine profile. See Azure confidential VMs for information on preparing confidential VM type master images and machine profiles.

5. On the **Storage and Licenses Types** page, select the storage and license type to be used as part of the image preparation process.

   NOTE:

   If you select a machine profile on the **Image** page, the license type of the machine profile is pre-selected based on the profile setting.

6. On the **Machine Specification** page, select a machine size. If you select a machine profile on the **Image** page, the machine size of the machine profile is selected by default.
7. On the **NICs** page, select or add NICs for the preparation image. For each NIC, select an associated virtual network.
8. On the **Disk Settings** page, select the customer-managed encryption key (CMEK). If the machine profile doesn't have a CMEK but the master image has, it pre-selects the CMEK from the master image.
9. On the **Image Definition** page, if you enable **Store image versions in Azure Compute Gallery**, the **Image Share** page appears, where you can select the resources with which to share the image version.
10. On the **Version Description** page, enter a description for the initial image version created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. On the **Summary** page, check the details of the image definition and the initial image version created. Enter a name and description for the image definition. Click **Finish**.

Create image versions

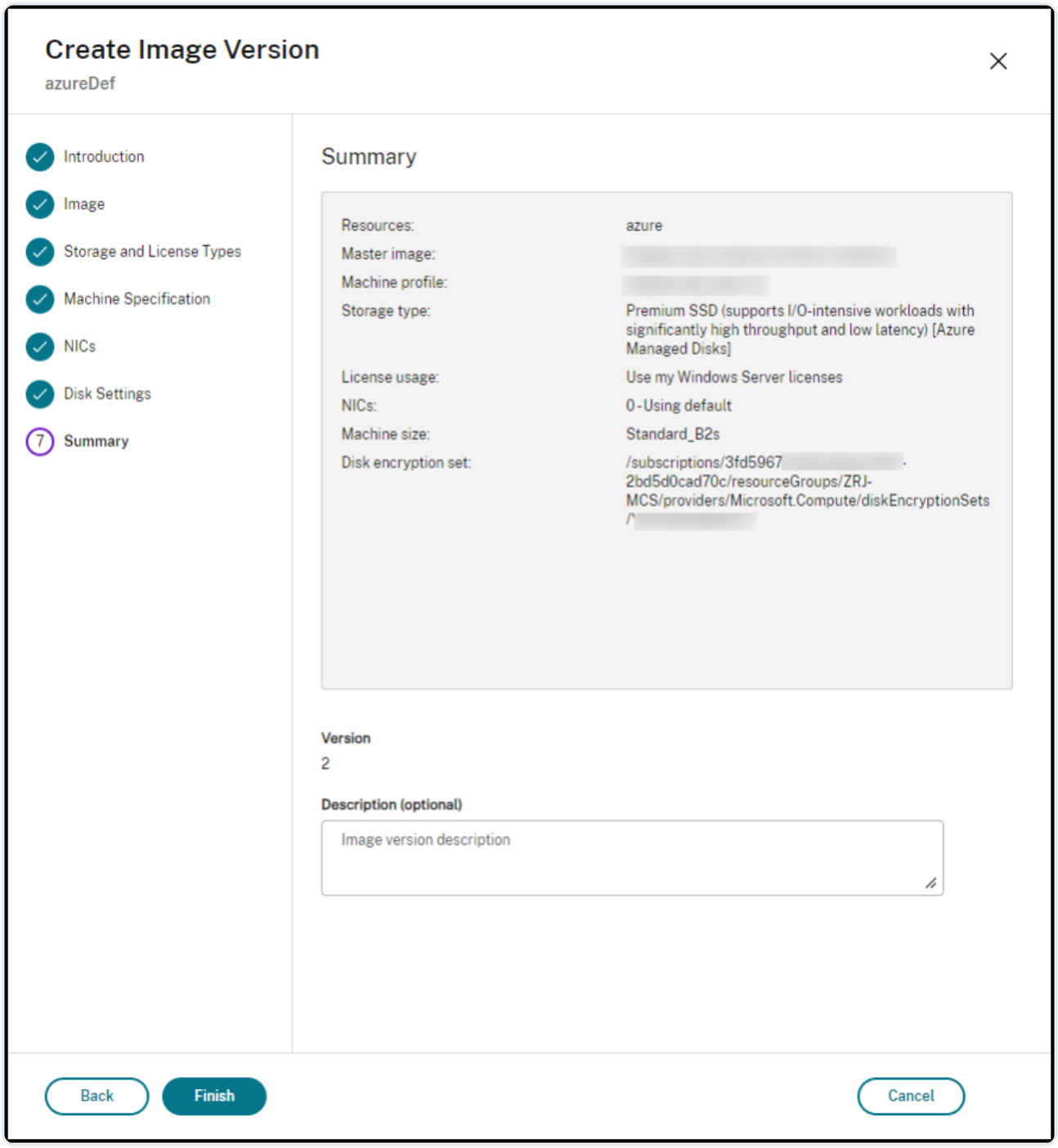
Image versions allow for the management of different iterations or updates to a particular image. This functionality enables you to maintain multiple versions of an image for different purposes.

To create image versions from the initial image version, do the following:

> **NOTE:**
>
> The hosting unit of all the image versions must be the same.

1. Go to the **Images** node, select an image version or an image definition, and click **Create Image Version**.
2. On the Image definition page, you can change the hosting unit, and reselect the master image and machine profile for that image version.
3. If you want the configuration of the image version to be different from the initial configured image version, then configure the settings on the **Storage and License Types**, **Machine Specification**, **NICs**, and **Disk Settings** pages of the **Create Image Version** dialog.
4. If the image definition enables **Store image versions in Azure Compute Gallery**, you can select the resources you want to share the image version with in the **Image Share** page.
5. Add a description for the image version. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

If the creation of the image version fails for any reason, the **Troubleshoot** tab at the bottom provides a **Retry** option.

Share prepared image

To share prepared images across different hosting units for Azure, follow these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Right-click an image version and select **Manage Image Share**. All hosting units in your Azure environment appear. The resources where the image version is created from is disabled for any actions.
2. Select the hosting units with which you want to share the image and click **Save**. The **Share Status** column shows **In progress**.
3. Click the **Resources** tab for more details about the sharing status.

NOTE:

When the status of the image version sharing is in progress, the option to **Delete Image Version** or **Manage Image Share** is disabled.

Create a machine catalog from the Images node

Use the **Create catalog** option in the **Images** node to create a catalog using the image version.

Alternatively, you can select the version when creating a catalog in the **Machine Catalogs** node, linking to the prepared image option in the catalog creation workflow. See Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the **Images** node, do the following:

1. Select an image version and click **Create catalog**. Click **Next** on the **Introduction** page.
2. On the **Desktop Experience** page, select the required desktop experience.
3. From the **Image** page to **Disk Settings** page, the settings are pre-selected based on the selected image version.
4. On the **Resource Group** page, you can choose to create a new resource group or use an existing resource group to place the resources of this catalog.
5. Complete the settings on the following pages.
6. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.
7. Go to the **Machine Catalogs** node to see the created machine catalog.

Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the **Machine Catalogs** node, do the following:

1. Click **Machine Catalogs** on the left navigation pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Create Machine Catalog**. The **Machine Catalog Setup** page appears. Click **Next** through the **Introduction** and **Machine Type** pages.
3. On the **Machine Management** page, select the following settings:
    a. Select **Machines that are power managed (for example, virtual machines or blade PCs).**
    b. Select **Citrix provisioning technology**. Then, select **Citrix Machine Creation Services™**.
    c. In the **Resources** field, the resources belonging to different zones are listed. Select any Azure network resource and click **Next**.
4. On the **Image** page: For Prepared image type, follow the steps:
    a. Select **Prepared image**.
    b. Under the **Prepared image**, select an image version of an image definition. If needed, add a note for the selected prepared image version.
    c. Click the image version name. To view more details about the selected image version, click the version number, which is underlined.
    d. If the selected image version is configured with a machine profile, select a machine profile. If the selected image version is not configured with a machine profile, you cannot choose to use a machine profile.
5. Configure the settings on the following pages.
6. On the **Disk Settings** page, if the selected prepared image uses a disk encryption set, then you cannot remove the encryption set, but you can change the key to another encryption key.
7. On the **Resource Group** page, you can choose to create a new resource group or use an existing resource group to place the resources of this catalog.
8. Complete the settings on the following pages.
9. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.

Use PowerShell

Create a prepared image

The detailed PowerShell commands to create a prepared image version spec are as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Check the available image definition names using the `Test-ProvImageDefinitionNameAvailable command`. For example,

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. Create an image definition using the `New-ProvImageDefinition` command. For example,

   ```
   New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
   -VdaSessionSupport MultiSession
   ```

3. Create a new configuration for image definition in the specified Hosting connection using the `Add-ProvImageDefinitionConnection` command.

   The `CustomProperties` for `Add-ProvImageDefinitionConnection` can include the following. If you do not use the parameters, then default values are used.

   - `ResourceGroups`: The resource group that has the base disks.
   - `UseSharedImageGallery`: Indicator for the type of base disks. Use `true` for ACG (image sharing) and `false` for snapshot.
   - `ImageGallery`: The gallery name when the base disk is an ACG image version.

   For example,

   - In case of snapshot and customer provided resource group:

     ```
     $CustomerOwnRsourceGroupProperties = @"

     <CustomProperties xmlns="http:// schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">

     <Property xsi:type="StringProperty" Name="ResourceGroups"
     Value="yangj_image" />

     </CustomProperties>

     "@
     ```

   - In case of ACG and customer provided resource group and image gallery:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$CustomerOwnAllProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

<Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />

</CustomProperties>

"@
```

- In case of ACG and customer provided resource group only:

```
$CustomerOwnResourceGroupProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

</CustomProperties>

"@
```

- In case of ACG and resource group and image gallery managed by Citrix:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$CustomerOwnResourceGroupNothingProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

</CustomProperties>

"@
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 [-CustomProperties $CustomProperties]
```

4. Create an image version using the `New-ProvImageVersion` command. For example,

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. Add a master image version spec to the image version using the `Add-ProvImageVersionSpec` command. For example,

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

NOTE:

You can add only one master image version spec to one image version for a hosting unit.

6. Create a prepared image version spec from the master image version spec using the `New-ProvImageVersionSpec` command.

   The CustomProperties for `New-ProvImageVersionSpec` can include the following. If you do not use the parameters, then default values are used:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `PreparedImageStorageType`: The storage type to use for the prepared image. Defaults to `Standard_LRS`, can also be `Premium_LRS` or `Standard_ZRS`. `Standard_ZRS` provides zone redundancy for the image.

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"}

-ServiceOffering"XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

7. You can also share a prepared image version spec with another hosting unit in all hosting connections by using the `Add-ProvImageVersionSpecHostingUnit` command.

   The CustomProperties for `Add-ProvImageVersionSpecHostingUnit` can include the following. If you do not use the parameters, then values from the source prepared image spec are used:

   - `PreparedImageStorageType`: The storage type to use for the prepared image.

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest
```

NOTE:

One hosting unit and preparation type can have only one prepared instance.

Example of the complete set of Powershell commands to create image definition, image version, and prepared image version spec:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession



$ImageDefinitionCustomProperties = @" <CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance"> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /> <Property
xsi:type="StringProperty" Name="ResourceGroups" Value="rg" /> <Property
xsi:type="StringProperty" Name="ImageGallery" Value="gallery" /> </
CustomProperties> "@



Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 -CustomProperties
$ImageDefinitionCustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid ` -HostingUnitUid
$hostingunit.HostingUnitUid ` -MasterImagePath "XDHyp:
\HostingUnits\azure28\image.folder\abc.resourcegroup\def-
snapshot.snapshot"



$ImageVersionSpecCustomProperties = @'



<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="PreparedImageStorageType"
Value="Premium_LRS" />



<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />



</CustomProperties>



'@



New-ProvImageVersionSpec -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network" } -CustomProperties
$ImageVersionSpecCustomProperties -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
-SourceImageVersionSpecUid $SourceImageVersionSpec.ImageVersionSpecUid



$TargetCustomProperties = @'



<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">



<Property xsi:type="StringProperty" Name="PreparedImageStorageType"
Value="Standard_ZRS" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</CustomProperties>



'@



Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest –TargetCustomProperties
$TargetCustomProperties



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

NOTE:

- All image version specs in an image definition must belong to the same hosting unit.
- An image version can have only one master image version spec and one prepared image version spec.
- All image version specs must either have a machine profile or none of the image version specs must have a machine profile.

Create a catalog using a prepared image version spec

Create an MCS machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<ProvisioningSchemeType>]

[-ImageAssignmentNote <string>]
```

Or,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]

[-ImageAssignmentNote <string>]
```

If you want to use an ACG image version spec, then set `UseSharedImageGallery` as `true`. For example,

```
$provSchemeCustomProperties= @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" />

</CustomProperties>

"@

New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -IdentityPoolUid $IdentityPool.IdentityPoolUid `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    -CleanOnBoot -Scope @() -SecurityGroup @() `

    -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
`

    -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network"} `

    -CustomProperties $provSchemeCustomProperties
```

Example of the complete set of Powershell commands to create a catalog:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">    <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /><Property
xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"StandardSSD_LRS`" /></CustomProperties>" -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Create Microsoft Entra joined and Microsoft Intune enrolled catalogs with prepared images

You can now use prepared images to create Microsoft Entra joined and Microsoft Intune enrolled catalogs. This feature is applicable to single and multi-session persistent and non-persistent type MCS catalogs. This implementation significantly reduces the storage and time costs, and simplifies the VM deployment and image update process.

EXAMPLES

- To create a Microsoft Entra catalog using a prepared image.

  ```
  New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
  <preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid>
  -IdentityPoolUid <IdentityPoolUid> [-CleanOnBoot] -NetworkMapping
  @{"0"="XDHyp:
  \HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.fol
  der\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<s
  unNetName>.network"} -ServiceOffering <serviceofferingPath> [-
  MachineProfile <machineProfilePath>] [-CustomProperties <>]
  ```

- To create a Microsoft Entra catalog enrolled in Microsoft Intune using a prepared image:

  ```
  New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
  <preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid>
  -IdentityPoolUid <IdentityPoolUid> [-CleanOnBoot] -NetworkMapping
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
@{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.fol
der\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<s
unNetName>.network"} -ServiceOffering <serviceofferingPath> [-
MachineProfile <machineProfilePath>] [-CustomProperties <>]
```

Share prepared images across Azure subscriptions or tenants

To share a prepared image across subscriptions or tenants on the Azure platform, follow this example:

- **Service principal**: SPN 1
- **Subscription**: Subscription 1
- **Tenant**: Tenant 1

You want to share this image with:

- **Service principal**: SPN 2
- **Subscription**: Subscription 2
- **Tenant**: Tenant 2 (can be the same as Tenant 1)

To successfully share and use the image, you must grant SPN 2 the following permissions in **Subscription 1**—at the gallery, resource group, or subscription scope:

- `Microsoft.Resources/subscriptions/read`
- `Microsoft.Compute/galleries/images/read`
- `Microsoft.Compute/galleries/images/versions/read`

> **NOTE:**
>
> Any service principal that has any permission on a subscription or resource automatically inherits the `Microsoft.Resources/subscriptions/read` permission.

Alternatively, assign the **Compute Gallery Image Reader** built-in role to **SPN 2**.

For step-by-step guidance, see this Microsoft article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Share encrypted prepared image across regions, subscriptions, and tenants

Azure Compute Gallery (ACG) images can be encrypted with a Disk Encryption Set (DES). With ACG sharing feature, you can share an encrypted prepared image across regions, subscriptions and tenants for Azure. The target resource needs to pick a DES in its region from the subscription where the prepared image belongs. You can thereafter create a machine catalog in the resource where the encrypted prepared image is shared.

The key steps to share an encrypted prepared image are:

1. Create Disk Encryption Set (DES) in each region: See the microsoft documentation Use the Azure portal to enable server-side encryption with customer-managed keys for managed disks.
2. Create an image definition for the Azure host connection and image versions in Azure Compute Gallery (ACG) and specify the DES to encrypt the prepared image : See Create an image definition and initial image version.
3. Share the encrypted prepared image across regions, subscriptions, and tenants: You can use Studio or PowerShell commands.

You can now create a machine catalog in the resource where the encrypted prepared image is shared. For more information on creating the catalog, see Create a prepared image machine catalog in Azure.

NOTE:

- If the primary region is not encrypted, the shared regions also cannot have DES.
- If two host units target the same region, they have the same DES.

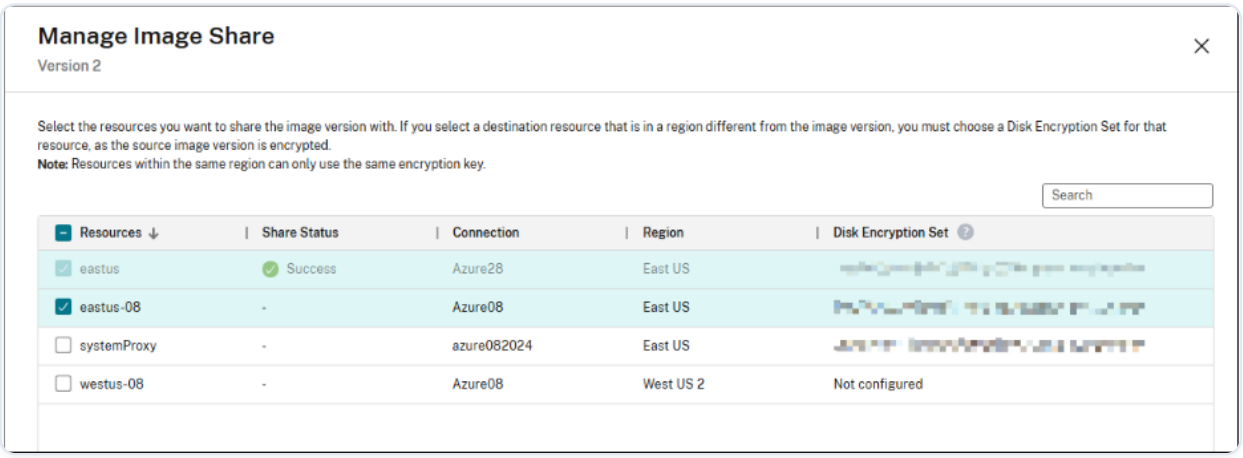
Share the encrypted image across regions, subscriptions, and tenants using Studio

1. Right-click an image version and select **Manage Image Share**. The resources with region and disk encryption set are listed.
2. Select the resources that you want to share with the image version. The resources where the image version is created from is disabled for any actions. Select a DES from the drop-down menu if DES is not configured for a resource.

   NOTE:

   Resources within the same region must use the same encryption key.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **Save**.
4. Click the **Resources** tab for more details about the sharing status.

NOTE:

- When the status of the image version sharing is in progress, the option to **Delete Image Version** or **Manage Image Share** is disabled.
- When a resource is successfully shared, the DES is not editable.

Share the encrypted image across regions, subscriptions, and tenants using PowerShell

Use the command `Add-ProvImageVersionSpecHostingUnit` and add the parameter `CustomProperties`. In `CustomProperties`, configure the DES for the target resource. When sharing the prepared encrypted image, each resource picks a DES in its region from the subscription which the prepared image belongs to. For example,

```
$CustomProperties = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">"

 "<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/xxxxxx-7152-46c4-b061-xxxxxx70c/resourceGroups/
resourcegroup1/providers/Microsoft.Compute/diskEncryptionSets/desid1`" /
>"+

 "</CustomProperties>"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <Guid>
-HostingUnitUid <Guid> -CustomProperties $CustomProperties
```

More information

- Image management

Where to go next

- Manage catalogs created using prepared images

Create catalogs using prepared images in Nutanix AHV Prism Central

Create prepared images and use the prepared images to create an MCS machine catalog using:

- PowerShell commands

The key steps to create an MCS machine catalog using the prepared image are:

1. Create the image definition and the initial image versions.
2. Use the image version as a prepared image to create a catalog

Use PowerShell

PowerShell example of image decoupling workflow in Nutanix PC.

Setting up

```
$CustomProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"><StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378"/></CustomProperties>'

$MasterImagePath="XDHyp:\HostingUnits\${HostingUnitName}
\Templates.folder\hai-vda-novtpm01.template\Initial
Version.templateversion"

$VMNetwork1A="XDHyp:\HostingUnits\${HostingUnitName}\Clusters.folder\mcs-
pvs-ntnx-cluster01.cluster\vmNwCl1-A.network"

$NetworkMapping=@{"0"=$VMNetwork1A}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create image definition and image version

```
$ImageDefinition = New-ProvImageDefinition -ImageDefinitionName
$ImgDefName -OsType Windows -VdaSessionSupport SingleSession

$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefinition.ImageDefinitionName -Description "V1"

Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefinition.ImageDefinitionName -HypervisorConnectionName
$HostingConnection
```

Create image version spec

```
$MasterImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName $HostingUnitName
-MasterImagePath $MasterImagePath

$ProvTask = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $MasterImageVersionSpec.ImageVersionSpecUid -NetworkMapping
$NetworkMapping -MachineProfile $MachineProfile -CustomProperties
$CustomProperties -AdditionalStorageIds
00062c6d-09a3-134b-446d-58a2e17d0f88 -RunAsynchronously

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
$ImgDefName -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

Create Provisioning Scheme

```
$ProvTask = New-ProvScheme -ProvisioningSchemeName $ProvSchemeName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName $HostingUnitName -IdentityPoolName $IdentityPoolName
-CleanOnBoot -Scope @() -SecurityGroup @() -NetworkMapping $NetworkMapping
-CustomProperties $CustomProperties -MachineProfile $MachineProfile
-RunAsynchronously
```

Replicate the image version spec to a new cluster

```
Add-ProvImageVersionSpecInstance -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -StorageID
00062c6d-09a3-134b-446d-58a2e17d0f88
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a new provisioning scheme in the new cluster using the same prepared image

```
$CustomProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"><StringProperty Name="ClusterId"
Value="00062c6d-09a3-134b-446d-58a2e17d0f88"/></CustomProperties>'

$ProvTask = New-ProvScheme -ProvisioningSchemeName $ProvSchemeName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-MachineProfile $MachineProfile -HostingUnitName $HostingUnitName
-IdentityPoolName $IdentityPoolName -CleanOnBoot -Scope @() -SecurityGroup
@() -NetworkMapping $NetworkMapping -CustomProperties $CustomProperties
-RunAsynchronously
```

More information

- Image management

Where to go next

- Manage catalogs created using prepared images

Create catalogs using prepared images in Red Hat OpenShift

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Studio
- PowerShell commands

The key steps to create an MCS machine catalog using the prepared image are:

1. Create the image definition and the initial image versions.
2. Use the image version as a prepared image to create a catalog

Use Studio

Create an image definition and initial image version

To create an image definition and the initial image version, do the following:

1. From Studio, go to the **Images** node, and click **Create Image Definition**. Click **Next** on the **Introduction** page.
2. On the **Image Definition** page, specify the **OS type** and **Session type** for the image definition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Image** page, select **Resources** (only the resources applicable for the set connection are listed) and a master image to use as a template for creating the image version. You can select the **Use a machine profile** checkbox and select a machine profile.

   NOTE:

   Before selecting an image, verify that the master image has VDA 2311 or later installed and the MCSIO driver is installed on the VDA.

4. On the **Machine Specification** page, select a machine size. If you select a machine profile, then you can see the Virtual CPU count derived from the machine profile and it is unchangeable. If you do not select a machine profile, then you can see only the memory size that is derived from the master image.
5. On the **NICs** page, select NICs for the preparation image. For each NIC, select an associated virtual network. The NIC associated with the hosting unit is selected by default.
6. On the **Version Description** page, enter a description for the initial image version created.
7. On the **Summary** page, check the details of the image definition and the initial image version created. Enter a name and description for the image definition. Click **Finish**.

Create image versions

Image versions allow for the management of different iterations or updates to a particular image. This functionality enables you to maintain multiple versions of an image for different purposes.

To create image versions from the initial image version, do the following:

1. Go to the **Images** node, select an image version or an image definition, and click **Create Image Version**.
2. On the **Image** page, you can reselect the master image for this image version.
3. If you want the configuration of the image version to be different from the initial configured image version, then configure the settings on the **Machine Specification** and **NICs** pages of the **Create Image Version** dialog.
4. Add a description for the image version. Click **Finish**.

NOTE:

If the creation of the image version fails for any reason, the **Troubleshoot** tab at the bottom provides a **Retry** option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a machine catalog from the Images node

Use the **Create catalog** option in the **Images** node to create a catalog using the image version.

Alternatively, you can select the version when creating a catalog in the **Machine Catalogs** node, linking to the prepared image option in the catalog creation workflow. See Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the **Images** node, do the following:

1. Select an image version and click **Create catalog**. Click **Next** on the **Introduction** page.
2. Click **Next** on the **Machine Management** page.
3. On the **Desktop Experience** page, select the required desktop experience.
4. From the **Image** page to **Virtual Machines** page, the settings are pre-selected based on the selected image version.
5. Complete the settings on the following pages.
6. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.
7. Go to the **Machine Catalogs** node to see the created machine catalog.

Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the **Machine Catalogs** node, do the following:

1. Click **Machine Catalogs** on the left navigation pane.
2. Click **Create Machine Catalog**. The **Machine Catalog Setup** page appears. Click **Next** through the **Introduction**, **Machine Type**, and **Machine Management** pages.
3. On the **Image** page:
    a. Select **Prepared image**.
    b. Under the **Prepared image**, select an image version of an image definition.
    c. Click the image version name. To view more details about the selected image version, click the version number, which is underlined.
4. Configure the settings on the following pages.
5. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use PowerShell

Create a prepared image

The detailed PowerShell commands to create a prepared image version spec are as follows:

1. Check the available image definition names using the `Test-ProvImageDefinitionNameAvailable command`. For example,

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. Create an image definition using the `New-ProvImageDefinition` command. For example,

   ```
   New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
   -VdaSessionSupport SingleSession
   ```

3. Create a new configuration for image definition in the specified Hosting connection using the `Add-ProvImageDefinitionConnection` command. For example,

   ```
   Add-ProvImageDefinitionConnection -ImageDefinitionUid
   $imageDef.ImageDefinitionUid -HypervisorConnectionUid
   "00000000-0000-0000-0000-000000000000"
   ```

4. Create an image version using the `New-ProvImageVersion` command. For example,

   ```
   New-ProvImageVersion -ImageDefinitionName
   $ImageDefintion.ImageDefinitionName -Description "version 1"
   ```

5. Add a master image version spec to the image version using the `Add-ProvImageVersionSpec` command. For example,

   ```
   Add-ProvImageVersionSpec -MasterImagePath "XDHyp:
   \HostingUnits\YourHostingUnitName\YourMasterImage.vm" -HostingUnitUid
   "11111111-1111-1111-1111-111111111111" -ImageVersionUid
   $imageVersion.ImageVersionUid
   ```

   NOTE:

   You can add only one master image version spec to one image version for a hosting unit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Create a prepared image version spec from the master image version spec using the `New-ProvImageVersionSpec` command. For example,

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
$masterImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"1" =
"XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetwo
rkAttachmentDefinition.network" }
```

Example of the complete set of Powershell commands to create image definition, image version, and prepared image version spec:

```
$imageDef = New-ProvImageDefinition -ImageDefinitionName "ImageDefinition"
-OsType "Windows" -VDASessionSupport "MultiSession"




$task = Add-ProvImageDefinitionConnection -ImageDefinitionUid
$imageDef.ImageDefinitionUid -HypervisorConnectionUid
"00000000-0000-0000-0000-000000000000"



$imageVersion = New-ProvImageVersion -ImageDefinitionName
"ImageDefinition"




$masterImageVersionSpec = Add-ProvImageVersionSpec -MasterImagePath
"XDHyp:\HostingUnits\YourHostingUnitName\YourMasterImage.vm"
-HostingUnitUid "11111111-1111-1111-1111-111111111111" -ImageVersionUid
$imageVersion.ImageVersionUid




$newProvImageVersionSpecResult = New-ProvImageVersionSpec
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-SourceImageVersionSpecUid $masterImageVersionSpec.ImageVersionSpecUid
-NetworkMapping @{"1" = "XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network" }
```

NOTE:

- All image version specs in an image definition must belong to the same hosting unit.
- An image version can have only one master image version spec and one prepared image version spec.
- All image version specs must either have a machine profile or none of the image version specs must have a machine profile.

Create a catalog using a prepared image version spec

Create an MCS machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
$getProvImageVersionSpecResult = Get-ProvImageVersionSpec
-ImageVersionSpecUid $newProvImageVersionSpecResult.ImageVersionSpecUid



New-ProvScheme -ImageVersionSpecUid
$newProvImageVersionSpecResult.ImageVersionSpecUid -ProvisioningSchemeName
"ProvSchemeImageDecoupling" -HostingUnitName "YourHostingUnitName"
-IdentityPoolName "YourIdentityPoolName" -NetworkMapping @{"1" = "XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network"}
```

More information

- Image management

Where to go next

- Manage catalogs created using prepared images

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create catalogs using prepared images in VMware

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Studio
- PowerShell commands

The key steps to create an MCS machine catalog using the prepared image are:

1. Create the image definition and the initial image versions.
2. Use the image version as a prepared image to create a catalog

Use Studio

Create an image definition and initial image version

To create an image definition and the initial image version, do the following:

1. From Studio, go to the **Images** node, and click **Create Image Definition**. Click **Next** on the **Introduction** page.
2. On the **Image Definition** page, specify the **OS type** and **Session type** for the image definition and **Connection** for the image definition.
3. On the **Image** page, select **Resources** (only the resources applicable for the set connection are listed) and a master image to use as a template for creating the image version. You can select the **Use a machine profile** checkbox and select a machine profile.

   NOTE:

   Before selecting an image, verify that the master image has VDA 2311 or later installed and the MCSIO driver is installed on the VDA.

4. On the **Machine Specification** page, select a machine size. If you select a machine profile, then you can see the Virtual CPU count derived from the machine profile and it is unchangeable. If you do not select a machine profile, then you can see only the memory size that is derived from the master image.
5. On the **NICs** page, select or add NICs for the preparation image. For each NIC, select an associated virtual network. If you do not select a machine profile, then the NIC associated with the master image is selected by default. If you select a machine profile, then the NICs are derived from the machine profile and the count is unchangeable.
6. On the **Version Description** page, enter a description for the initial image version created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. On the **Summary** page, check the details of the image definition and the initial image version created. Enter a name and description for the image definition. Click **Finish**.

Create image versions

Image versions allow for the management of different iterations or updates to a particular image. This functionality enables you to maintain multiple versions of an image for different purposes.

To create image versions from the initial image version, do the following:

1. Go to the **Images** node, select an image version or an image definition, and click **Create Image Version**.
2. On the **Image** page, you can change the hosting unit within the same hosting connection, and reselect the master image and machine profile for that image version.
3. If you want the configuration of the image version to be different from the initial configured image version, then configure the settings on the **Machine Specification** and **NICs** pages of the **Create Image Version** dialog.
4. Add a description for the image version. Click **Finish**.

NOTE:

If the creation of the image version fails for any reason, the **Troubleshoot** tab at the bottom provides a **Retry** option.

Share prepared images

PREREQUISITES

Share prepared images replicates images across vCenter Server instances using cold migration. The following prerequisites apply to the hosting units belonging to different hosting connections:

- Cloud Connector to target vCenter Connectivity: The source Resource Location Cloud Connector must have HTTPS access (port 443) to the target vCenter. Replication fails if the source connector can't establish a vSphere SDK connection to coordinate the operation.

SOURCE	DESTINATION	PORT	PROTOCOL	PURPOSE
Source Cloud Connector	Target vCenter Server	443	TCP	vSphere SDK management connection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cold migration between vCenter Servers: Cold migration requires cross-vCenter migration support in both environments.
  - Both vCenter Servers must run vSphere 7.0 or later (vSphere 8.0+ recommended).
  - Enhanced linked mode is not required.

  Port requirement: Ensure the following ports are open for migration:

SOURCE	DESTINATION	PORT	PROTOCOL	PURPOSE
Source vCenter Server	Target vCenter Server	443	TCP	API communication between vCenters
Source ESXi Host	Target ESXi Host	902	TCP	NFC (Network File Copy) data transfer
Source ESXi Host	Target ESXi Host	8000	TCP	vMotion traffic

NOTE:

Ports must be open bidirectionally. Migration primarily uses NFC (port 902) for data and port 443 for management. Port 8000 may be used depending on the path. The source vCenter must validate the target's SSL certificate thumbprint during the clone operation.

VMkernel adapter configuration:

ESXI HOST	REQUIRED SERVICE
Source ESXi Host	Provisioning or Management
Target ESXi Host	Same service as source (Provisioning or Management)

Both sides must enable the same traffic service (Provisioning or Management) on VMkernel adapters. Mismatches cause migration failure.

Verify in the vSphere Client under **Host > Configure > Networking > VMkernel adapters**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known limitation: Custom storage policies are not preserved during cross-vCenter replication. The default storage policy of the target datastore is applied.

- vTPM-enabled machine profile: Key provider compatibility. For profiles with vTPM, both vCenter Servers must access a compatible Key Provider.

REQUIREMENT	DETAIL
Same Key Provider access	The destination vCenter must have access to the same key provider as the source, or use the Native Key Provider as a bridge
Key material	For external KMS: both vCenters must be enrolled to the same KMS cluster (or a KMS cluster that shares key material)
Native Key Provider	Configure a Native Key Provider on both vCenter Servers. Each vCenter's Native Key Provider is independent, but vSphere accepts this combination for cross-vCenter operations. The Native Key Provider can also act as a bridge if the source and destination do not share an external KMS. The Native Key Provider must be backed up on both vCenters before use.

NOTE:

The Native Key Provider is the simplest option. Configure and back it up on both servers. If using external KMS, ensure both vCenters share the same cluster or key material. Verify Key Provider configuration in the **vSphere Client under vCenter > Configure > Security > Key Providers before enabling image sharing for vTPM-enabled catalogs**.

SHARE PREPARED IMAGES ACROSS DIFFERENT HOST UNITS

To share prepared images across different host units, follow these steps:

1. Right-click an image version and select **Manage Image Share**. All hosting units in your VMware environment appear. The resources where the image version is created from is disabled for any actions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the hosting units with which you want to share the image and click **Save**. The **Share Status** column shows **In progress**.
3. Click the **Resources** tab at the bottom for more details about the sharing status.

NOTE:

When the status of the image version sharing is in progress, the option to **Delete Image Version** or **Manage Image Share** is disabled. To share an image with a hosting unit in a different VMware connection, ensure the following requirements are met:

- The two connections can communicate with each other. The hypervisor versions are consistent.
- The Provisioning services are enabled on management VMkernel adapters of both the source and target hosts. The **Host > Configure > Networking > VMkernel adapters** is the navigation path in the VMware vSphere Client.

Create a machine catalog from the Images node

Use the **Create catalog** option in the **Images** node to create a catalog using the image version.

Alternatively, you can select the version when creating a catalog in the **Machine Catalogs** node, linking to the prepared image option in the catalog creation workflow. See Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the **Images** node, do the following:

1. Select an image version and click **Create catalog**. Click **Next** on the **Introduction** page.
2. On the **Desktop Experience** page, select the required desktop experience.
3. From the **Image** page to **Virtual Machines** page, the settings are pre-selected based on the selected image version.
4. Complete the settings on the following pages.
5. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.
6. Go to the **Machine Catalogs** node to see the created machine catalog.

Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the **Machine Catalogs** node, do the following:

1. Click **Machine Catalogs** on the left navigation pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Create Machine Catalog**. The **Machine Catalog Setup** page appears. Click **Next** through the **Introduction**, **Machine Type**, and **Machine Management** pages.
3. On the **Image** page:
   a. Select **Prepared image**.
   b. Under the **Prepared image**, select an image version of an image definition. If needed, add a note for the selected prepared image version.
   c. Click the image version name. To view more details about the selected image version, click the version number, which is underlined.
   d. If the selected image version is configured with a machine profile, select a machine profile. If the selected image version is not configured with a machine profile, you cannot choose to use a machine profile.
4. Configure the settings on the following pages.
5. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.

Use PowerShell

Create a prepared image

The detailed PowerShell commands to create a prepared image version spec are as follows:

1. Check the available image definition names using the `Test-ProvImageDefinitionNameAvailable command`. For example,

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. Create an image definition using the `New-ProvImageDefinition` command. For example,

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. Create a new configuration for image definition in the specified Hosting connection using the `Add-ProvImageDefinitionConnection` command. For example,

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Create an image version using the `New-ProvImageVersion` command. For example,

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. Add a master image version spec to the image version using the `Add-ProvImageVersionSpec` command. For example,

```
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware
-MasterImagePath $MasterImagePath
```

> **NOTE:**
>
> You can add only one master image version spec to one image version for a hosting unit.

6. Create a prepared image version spec from the master image version spec using the `New-ProvImageVersionSpec` command. For example,

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. You can also share a prepared image version spec with another hosting unit within the same hosting connection using the `Add-ProvImageVersionSpecHostingUnit` command. For example,

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc
```

Example of the complete set of Powershell commands to create image definition, image version, and prepared image version spec:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport Single



Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware



$imageVersion = New-ProvImageVersion -ImageDefinitionName image2



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\vmware\shuaiz-win10-
master.vm\shuaiz-win10-master-snap.snapshot"



New-ProvImageVersionSpec -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-
VMNetwork.network"} `

    -VMCpuCount 2 -VMMemoryMB 4096







Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc

 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- All image version specs in an image definition must belong to the same hosting unit.
- An image version can have only one master image version spec and one prepared image version spec.
- All image version specs must either have a machine profile or none of the image version specs must have a machine profile.

Create a catalog using a prepared image version spec

Create an MCS machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]

[-ImageAssignmentNote <string>]
```

Or,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]

[-ImageAssignmentNote <string>]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example of creating a catalog using a prepared image version spec in VMware:

```
New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitName $hostingunit.c-IdentityPoolName
$IdentityPool.IdentityPoolName `

    -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM
Network.network"}
```

Example of the complete set of Powershell commands to create a catalog:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

More information

- Image management

Where to go next

- Manage catalogs created using prepared images

Create catalogs using prepared images in XenServer®

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Studio
- PowerShell commands

The key steps to create an MCS machine catalog using the prepared image are:

1. Create the image definition and the initial image versions.
2. Use the image version as a prepared image to create a catalog

Use Studio

Create an image definition and initial image version

To create an image definition and the initial image version, do the following:

1. From Studio, go to the **Images** node, and click **Create Image Definition**. Click **Next** on the **Introduction** page.
2. On the **Image Definition** page, specify the **OS type** and **Session type**, and **Connection** for the image definition.
3. On the **Image** page, select **Resources** (only the resources applicable for the set connection are listed) and a master image to use as a template for creating the image version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Before selecting an image, verify that the master image has VDA 2311 or later installed and the MCSIO driver is installed on the VDA.

4. On the **Machine Specification** page, you can see only the memory size that is derived from the master image, and you can change it if needed.
5. On the **NICs** page, select NICs for the preparation image. For each NIC, select an associated virtual network. The NIC associated with the master image is selected by default.
6. On the **Version Description** page, enter a description for the initial image version created.
7. On the **Summary** page, check the details of the image definition and the initial image version created. Enter a name and description for the image definition. Click **Finish**.

Create image versions

Image versions allow for the management of different iterations or updates to a particular image. This functionality enables you to maintain multiple versions of an image for different purposes.

To create image versions from the initial image version, do the following:

1. Go to the **Images** node, select an image version or an image definition, and click **Create Image Version**.
2. On the **Image** page, change the hosting unit, and reselect the master image if needed.
3. To use different settings from the initial image version, configure the settings on the **Machine Specification** and **NICs** pages in the **Create Image Version** dialog.
4. Add a description for the image version. Click **Finish**.

NOTE:

If the creation of the image version fails for any reason, the **Troubleshoot** tab at the bottom provides a **Retry** option.

Shared prepared image

To share prepared images across different host units for Xenserver, follow these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Right-click an image version and select **Manage Image Share**. All the host units under the selected connection are listed. The resources where the image version is created from is disabled for any actions.
2. Select the host units with which you want to share the image and click **Save**. The **Share Status** column shows **In progress**.
3. Click the **Resources** tab for more details about the sharing status.

NOTE:

When the status of the image version sharing is in progress, the option to delete image version or manage image share is disabled.

Create a machine catalog from the Images node

Use the **Create catalog** option in the **Images** node to create a catalog using the image version.

Alternatively, you can select the version when creating a catalog in the **Machine Catalogs** node, linking to the prepared image option in the catalog creation workflow. See Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the **Images** node, do the following:

1. Select an image version and click **Create catalog**. Click **Next** on the **Introduction** page.
2. On the **Machine Management** page, select the hosting unit and click **Next**.
3. On the **Desktop Experience** page, select the required desktop experience.
4. From the **Image** page to the **Virtual Machines** page, settings are pre-selected based on the selected image version.
5. Complete the settings on the following pages.
6. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.
7. Go to the **Machine Catalogs** node to see the created machine catalog.

Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the **Machine Catalogs** node, do the following:

1. Click **Machine Catalogs** on the left navigation pane.
2. Click **Create Machine Catalog**. The **Machine Catalog Setup** page appears. Click **Next** through the **Introduction**, **Machine Type**, and **Machine Management** pages.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Image** page:
    a. Select **Prepared image**.
    b. Under the **Prepared image**, select an image version of an image definition.
    c. Select the image version. To view more details about the selected image version, click the version number, which is underlined.
4. Complete the settings on the following pages.
5. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.

Use PowerShell

Create a prepared image

The detailed PowerShell commands to create a prepared image version spec are as follows:

1. Check the available image definition names using the `Test-ProvImageDefinitionNameAvailable command`. For example,

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName xenimage1
```

2. Create an image definition using the `New-ProvImageDefinition` command. For example,

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName
xenimage1 -OsType Windows -VdaSessionSupport SingleSession
```

3. Create a new configuration for image definition in the specified Hosting connection using the `Add-ProvImageDefinitionConnection` command.

```
Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName
XenServer1
```

4. Create an image version using the `New-ProvImageVersion` command. For example,

```
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Add a master image version spec to the image version using the `Add-ProvImageVersionSpec` command. For example,

```
$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName $ImageDefintion.ImageDefinitionName -ImageVersionNumber $ImageVersion.ImageVersionNumber -HostingUnitName xenhu -MasterImagePath $MasterImagePath
```

> **NOTE:**
>
> You can add only one master image version spec to one image version for a hosting unit.

6. Create a prepared image version spec from the master image version spec using the `New-ProvImageVersionSpec` command. For example,

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}

-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. You can also share prepared image version spec with another hosting unit within the same hosting connection using the `Add-ProvImageVersionSpecHostingUnit` command. For example,

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx -HostingUnitName xenhu2
```

Example of the complete set of Powershell commands to create image definition, image version, and prepared image version spec:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName xenimage1 -OsType Windows -VdaSessionSupport SingleSession
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName XenServer1



$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"



$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-
master-snap.snapshot"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName xenhu -MasterImagePath
$MasterImagePath




New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\xenhu\VM Network.network"}

 -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously



Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName xenhu2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- An image version can have only one master image version spec and one prepared image version spec.
- All image version specs must either have a machine profile or none of the image version specs must have a machine profile.

Create a catalog using a prepared image version spec

Create an MCS machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

Or,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

Example of creating a catalog using a prepared image version spec in XenServer:

```
New-ProvScheme -ProvisioningSchemeName assignimage -imageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid 1 `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -HostingUnitName xenhu -IdentityPoolName poo1 `

  -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
```

Example of the complete set of Powershell commands to create a catalog:

```
$CatalogName = "XenCatalog"

$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" `

  -Name $CatalogName -PersistUserChanges "Discard" -ProvisioningType "MCS"
-Scope @() -SessionSupport "MultiSession"




$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "xen.local"
-IdentityPoolName $CatalogName `

  -IdentityType "ActiveDirectory"  -NamingScheme "xen##" -NamingSchemeType
"Numeric" -Scope @()




$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
xenimage1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"




$Task = New-ProvScheme -ProvisioningSchemeName $CatalogName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid `

  -HostingUnitName xenhu -IdentityPoolName $CatalogName -CleanOnBoot
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-Scope @() -SecurityGroup @() `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName $CatalogName




Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

More information

- Image management

Where to go next

- Manage catalogs created using prepared images

Manage catalogs created using prepared images

You can update an existing MCS machine catalog with a different prepared image and manage the image definitions and versions using:

- Studio
- PowerShell

Use Studio

Update a machine catalog with a different prepared image

To update an existing MCS machine catalog with a different prepared image, do the following:

1. Click **Machine Catalogs** in the left pane and select a machine catalog that you want to update. Right-click and select **Change Prepared Image**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the **Image** page, select a prepared image. If needed, add a note for the selected prepared image.

   NOTE:

   (Azure only) You can also choose an image with ACG not enabled and later select **Place prepared image in Azure Compute Gallery** check box to place the images in the gallery.

3. To roll back to a previously assigned prepared image, click **Use previous image assignment for quick rollback** at the bottom of the wizard.

   A new window opens and displays a list of all available historical image assignments. When you select an image from the list, the corresponding version is automatically selected in the prepared image tree on the image page.

4. On the **Rollout strategy** page, select when you want to update this catalog with the selected prepared image.
5. On the **Summary** page, check the details. Click **Finish**.

To view the history of image changes made to a catalog, follow these steps:

1. Select a machine catalog.
2. Under the **Template Properties** tab in the **Prepared image** field, click **View Image history**.

Manage the image definitions and versions

You can edit and delete the image definitions and versions to manage the use of various created image versions and definitions.

EDIT AN IMAGE DEFINITION

You can edit the name and description of an image definition.

To edit an image definition, do the following:

1. Go to the **Images** node, select an image definition, and select **Edit Image Definition**.

EDIT IMAGE VERSION

You can edit the description of an image version to specify the purpose of that image version.

To edit an image version, do the following:

1. Go to the **Images** node, select an image version, and select **Edit Description**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DELETE AN IMAGE VERSION

To delete an image version, do the following:

1. Go to the **Images** node, select an image version, and select **Delete Image Version**.

> **NOTE:**
>
> You cannot delete an image version if it is used by a machine catalog.

DELETE AN IMAGE DEFINITION

To delete an image definition, do the following:

1. Go to the **Images** node, select an image definition, and select **Delete Image Definition**.

> **NOTE:**
>
> You cannot delete an image definition if it contains an image version.

Use PowerShell

Update a catalog using a prepared image version spec

You can update a catalog using the `Set-ProvSchemeImage` command. For example,

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]

[-ImageAssignmentNote <string>]
```

Or,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]

[-ImageAssignmentNote <string>]
```

Example of the complete set of Powershell commands to update a catalog:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"



Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously -ImageAssignmentNote "Update from VST team"
```

Get the image change history for the provisioning scheme

```
Get-ProvSchemeImageVersionSpecHistory -ProvisioningSchemeName azurecatalog
```

Delete image definition, image version, and prepared image version spec

Consider the following before deleting an image definition, image version, and prepared image version spec:

- An image definition can't be deleted if it contains any image version.
- An image version can't be deleted if it contains any image version specification.
- A master image version spec can't be deleted if it is used by any other prepared image version spec.
- A prepared image version spec can't be deleted if it is used by any MCS machine catalog.
- A hosting unit can’t be deleted if it is used by any other prepared image version spec.

The detailed steps are as follows:

1. Remove the machine catalog. For example,

   ```
   Remove-ProvScheme -ProvisioningScheneName decouplingCatalog
   ```

2. Remove the shared prepared image version spec. For example,

   ```
   Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>
   -HostingUnitName AzureWest
   ```

3. Remove a prepared image version spec. For example,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec
-ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
"PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

4. Remove master image version specification. For example,

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronousl
```

NOTE:

Master image version spec can only be deleted when there is no associated prepared image version spec.

5. Remove an image version. For example,

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

6. Remove the configuration for image definition in the specified hosting connection. For example,

```
Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx
```

7. Remove an image definition. For example,

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example of the complete set of PowerShell commands when prepared image is not shared across host unit:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinition -ImageDefinitionName image1
```

Example of the complete set of PowerShell commands when prepared image is shared across host unit:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-HostingUnitName AzureWest



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx



Remove-ProvImageDefinition -ImageDefinitionName image1
```

Manage image definition and image version

You can rename and edit an image definition, and edit an image version.

- Rename an image definition using the `Rename-ProvImageDefinition` command. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
-NewImageDefinitionName <string>
```

Or,

```
Rename-ProvImageDefinition -ImageDefinitionName <string>
-NewImageDefinitionName <string>
```

- Edit an image definition using the `Set-ProvImageDefinition` command. For example:

```
Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
<string>]
```

Or,

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
<string>]
```

- Edit an image version using the `Set-ProvImageVersion` command. For example:

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

Or,

```
Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
<int> [-Description <string>]
```

Get image definition, image version, prepared image version spec, and provisioning scheme details

- Get image definition details using the `Get-ProvImageDefinition` command. For example:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- Get image version details using the `Get-ProvImageVersion` command. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - To list image versions in an image definition,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    Or,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - To get an image version detail,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    Or,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    -ImageVersionNumber <int>
    ```

- Get prepared image version spec using the `Get-ProvImageVersionSpec` command. For example:

  - To list all prepared image version specs in an image version,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    ```

  - To list master image version specs in a prepared image version spec,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
    'PreparationType -eq "None"'
    ```

  - To list prepared image version specs in an image version, which is associated with a master image,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
    'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
    "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
    ```

  - To get successful prepared image version specs in an image version,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
-eq "Complete"'
```

- To get a prepared image version spec detail,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- Get provisioning scheme details using the `Get-ProvScheme` command. For example:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- Get prepared image version spec history of a provisioning scheme using the `Get-ProvSchemeImageVersionSpecHistory` command. For example:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

More information

- Image management

Create machine catalogs

NOTE:

This article describes how to create catalogs using Studio. If you're using Quick Deploy to create Azure resources, follow the guidance in Create catalogs using Quick Deploy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Collections of physical or virtual machines are managed as a single entity called a machine catalog. Within a machine catalog, all machines share a common operating system type, which can be either multi-session OS or single-session OS, such as Windows or Linux-based systems.

NOTE:

For more information about provisioning macOS machines using machine catalogs, see this article in the macOS VDA documentation.

Studio guides you to create the first machine catalog. After you create the first catalog, you create the first delivery group. Later, you can change the catalog you created, and create more catalogs.

Overview

When you create a catalog of VMs, you specify how to provision those VMs. You can use Machine Creation Services™ (MCS). Or, you can use your own tools to provide machines.

- If you use MCS to provision VMs, you provide an image (or snapshot) to create identical VMs in the catalog. Before you create the catalog, you must set up a hosting connection for the first time to the hypervisor or cloud service of choice and then you must create and configure the master image on the same. Configuring the master image requires tasks such as domain joining when necessary, installing required drivers, applications to be published, and deploying the Virtual Delivery Agent (VDA) on the image.
- After you create the master image, you then create the machine catalog in Studio. You select that image (or a snapshot of an image), specify the number of VMs to create in the catalog, and configure additional information.
- If your machines are already available, you must still create one or more machine catalogs to import these VMs into the catalog.

When using MCS to create the first catalog, you specify a hosting unit that you created previously. Hosting unit provide resource configuration for you to create a virtual machine. Later (after you create your first catalog and delivery group), you can change information about that hosting unit or its parent host connection or create more connections and hosting units.

If a Cloud Connector is not operating properly, MCS provisioning operations (such as catalog updates) take longer than usual, and the management interface's performance degrades significantly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RDS license check

Creation of a machine catalog containing Windows multi-session OS machines includes an automatic check for valid Microsoft RDS licenses. The catalog is searched for a powered-on and registered machine to do the check on.

- If a powered-on and registered machine cannot be found, a warning is displayed, explaining that the RDS licensing check cannot be performed.
- If a machine is found and an error is detected, Studio displays a warning message for the catalog containing the detected issue. To remove an RDS license warning from a catalog (so that it no longer appears in the display), select the catalog. Select **Remove RDS license warning**. When prompted, confirm the action.

VDA registration

A VDA must be registered with a Cloud Connector to be considered when launching brokered sessions. Unregistered VDAs can result in underutilization of otherwise available resources. There are various reasons that a VDA might not be registered, many of which you can troubleshoot. Troubleshooting information is provided in the catalog creation wizard, and after you add a catalog to a delivery group.

In the catalog creation wizard, after you add existing machines, the list of computer account names indicates whether each machine is suitable for adding to the catalog. Hover over the icon next to each machine to display an informative message about that machine.

If the message identifies a problematic machine, you can either remove that machine (using the **Remove** button), or add the machine. For example, if a message indicates that information cannot be obtained about a machine (perhaps because it was never registered), you might choose to add the machine anyway.

For more information about VDA registration troubleshooting, see CTX136668.

MCS catalog creation summary

Here's a brief overview of default MCS actions after you provide information in the catalog creation wizard.

- If you select an image (rather than a snapshot), MCS creates a snapshot.
- MCS creates a full copy of the snapshot and places the copy on each storage location defined in the host connection.
- MCS adds the machines to Active Directory, which creates unique identities.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- MCS creates the number of VMs specified in the wizard, with two disks defined for each VM. In addition to the two disks per VM, full copy of the snapshot or master image is also stored in the same storage location. If you have multiple storage locations defined, each gets the following disk types:
  - The full copy of the snapshot (noted before), which is read-only and shared across the just-created VMs.
  - A unique 16 MB identity disk that gives each VM a unique identity. Each VM gets an identity disk.
  - A unique difference disk to store writes made to the VM. This disk is thin provisioned (if supported by the host storage) and increases to the maximum size of the master image, if necessary. Each VM gets a differencing disk. The difference disk holds changes made during sessions. It is permanent for dedicated desktops. For pooled desktops, it is deleted and a new one created after each restart.
- For Windows VMs on VDA version 2511 (Update 1) or later, MCS can assign a unique `MachineGuid` to each machine. This `MachineGuid` is used for licensing purposes by some software installed on the VDA. This behavior is disabled by default but can be enabled by setting registry key value `HKLM:\Software\Citrix\MachineIdentityServiceAgent\EnableUniqueMachineGuid` to `1` on the master image or individual machines.

Alternatively, when creating VMs to deliver static desktops, you can specify (on the **Machines** page of the catalog creation wizard) thick (full copy) VM clones. Full clones do not require retention of the master image on every data store. Each VM has its own file.

MCS storage considerations

There are many factors when deciding on storage solutions, configurations, and capacities for MCS. The following information provides proper considerations for storage capacity:

Capacity considerations:

- Disks

  The Delta or Differencing (Diff) Disks consume the largest amount of space in most MCS deployments for each VM. Each VM created by MCS is given at minimum 2 disks upon creation.

  - Disk0 = Diff Disk: contains the OS when copied from the base master image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Disk1 = Identity Disk: 16 MB - contains Active Directory data for each VM.

As the product evolves, you might have to add more disks to satisfy certain use cases and feature consumption. For example:

- MCS Storage Optimization creates a write cache style disk for each VM. In XenServer, VMware, and SCVMM virtualization environments, MCS places Write-back cache (WBC) disk on the same storage location as OS disk if you configure the available OS storage list the same as the available temporary storage list while creating a host connection.
- MCS added the ability to use full clones as opposed to the Delta disk scenario described in the previous section.

Hypervisor features might also enter into the equation. For example:

- XenServer IntelliCache creates a Read Disk on local storage for each XenServer. This option saves on IOPS against the image which might be held on the shared storage location.

- Hypervisor overhead

  Different hypervisors use specific files that create overhead for VMs. Hypervisors also use storage for management and general logging operations. Calculate the space to include overhead for:

  - Log files
  - Hypervisor-specific files. For example:
    - VMware adds more files to the **VM storage** folder. See VMware Best Practices.
    - Calculate your total virtual machine size requirements. Consider a virtual machine containing 20 GB for the virtual disk, 16 GB for the swap file, and 100 MB for log files consuming 36.1 GB total.
  - Snapshots for XenServer; Snapshots for VMware.

- Process overhead

  Creating a catalog, adding a machine, and updating a catalog have unique storage implications. For example:

  - Initial catalog creation requires a copy of the base disk to be copied to each storage location.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Adding a machine to a catalog does not require copying of the base disk to each storage location. Catalog creation varies based on the features selected.
- Updating the catalog to create an extra base disk on each storage location. Catalog updates also experience a temporary storage peak where each VM in the catalog has 2 Diff disks for a certain amount of time.

More considerations:

- **RAM sizing:** Affects the size of certain hypervisor files and disks, including I/O optimization disks, write cache, and snapshot files.
- **Thin / Thick provisioning:** NFS storage is preferred due to the thin provisioning capabilities.

Machine Creation Services (MCS) storage optimization

The Machine Creation Services (MCS) storage optimization feature is also known as MCS I/O. This feature is only available on Azure, GCP, XenServer, VMware, AWS, and SCVMM.

- The write-cache container is *file-based*, the same functionality found in Citrix Provisioning. For example, the Citrix Provisioning write cache file name is `D:\vdiskdif.vhdx` and the MCS I/O write cache file name is `D:\mcsdif.vhdx`.
- Achieve diagnostic improvements by including support for a Windows crash dump file written to the write-cache disk.
- MCS I/O retains the technology *cache in RAM with overflow to hard disk* to provide the most optimal multi-tier write cache solution. This functionality allows an administrator to balance between the cost in each tier, RAM and disk, and performance to meet the desired workload expectation.

Updating the write cache method from *disk-based* to *file-based* requires the following changes:

1. MCS I/O no longer supports RAM only cache. Specify a disk size during machine catalog creation.
2. The VM write cache disk is created and formatted automatically when booting a VM for the first time. Once the VM is up, the write cache file `mcsdif.vhdx` is written into the formatted volume `MCSWCDisk`.
3. The pagefile is redirected to this formatted volume, `MCSWCDisk`. As a result, this disk size considers the total amount of disk space. It includes the delta between the disk size and the generated workload plus the pagefile size. This is typically associated with VM RAM size.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable MCS storage optimization updates

To enable the MCS I/O storage optimization feature, upgrade the Cloud Connector and the VDA to the latest version of Citrix DaaS.

NOTE:

If you upgrade an existing deployment which has MCS I/O enabled, no additional configuration is required. The VDA and the Delivery Controller upgrade handle the MCS I/O upgrade.

For information on assigning a drive letter to write-back cache disk, see Assign a specific drive letter to MCS I/O write-back cache disk.

Prepare a master image on the hypervisor or cloud service

The master image contains the operating system, non-virtualized applications, VDA, and other software.

Good to know:

- A master image might also be known as a clone image, golden image, base VM, or base image. Host vendors and cloud service providers might use different terms.
- Ensure that the hypervisor or cloud service has enough processors, memory, and storage to accommodate the number of machines created.
- Configure the correct amount of hard disk space needed for desktops and applications. That value cannot be changed later or in the machine catalog.
- Remote PC Access machine catalogs do not use master images.
- Microsoft KMS activation considerations when using MCS: If your deployment includes 7.x VDAs with a XenServer 6.1 or 6.2, vSphere, or Microsoft System Center Virtual Machine Manager host, you do not need to manually rearm Microsoft Windows or Microsoft Office.

Install and configure the following software on the master image:

- Integration tools for your hypervisor (such as Citrix VM Tools, Hyper-V Integration Services, or VMware tools). If you omit this step, applications and desktops might not function correctly.
- A VDA. Citrix recommends installing the latest version of VDA to allow access to the newest features. Failure to install a VDA on the master image causes the catalog creation to fail.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Third-party tools as needed, such as antivirus software or electronic software distribution agents. Configure services with settings that are appropriate for users and the machine type (such as updating features).
- Third-party applications that you are not virtualizing. Citrix recommends virtualizing applications. Virtualizing reduces costs by eliminating having to update the master image after adding or reconfiguring an application. Also, fewer installed applications reduce the size of the master image hard disks, which saves storage costs.
- App-V clients with the recommended settings, if you plan to publish App-V applications. The App-V client is available from Microsoft.
- When using MCS, if you localize Microsoft Windows, install the locales and language packs. During provisioning, when a snapshot is created, the provisioned VMs use the installed locales and language packs.

IMPORTANT:

If you are using MCS, do not run Sysprep on master images.

To prepare a master image:

1. Using your hypervisor's management tool, create a master image and then install the operating system, and all service packs and updates. Specify the number of vCPUs. You can also specify the vCPU value if you create the machine catalog using PowerShell. You cannot specify the number of vCPUs when creating a catalog from Studio. Configure the amount of hard disk space needed for desktops and applications. That value cannot be changed later or in the catalog.
2. Ensure that the hard disk is attached at device location 0. Most standard master image templates configure this location by default, but some custom templates might not.
3. Install and configure the software listed above on the master image.
4. If you are not using MCS, join the master image to the domain where applications and desktops are members. Ensure that the master image is available on the host where the machines are created. If you are using MCS, joining the master image to a domain is not required. The provisioned machines are joined to the domain specified in the catalog creation wizard.
5. Citrix recommends that you create and name a snapshot of your master image so that it can be identified later. If you specify a master image rather than a snapshot when creating a catalog, the management interface creates a snapshot, but you cannot name it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Volume licensing activation

MCS supports volume licensing activation to automate and manage the activation of Windows operating systems and Microsoft Office. The three models that MCS supports for volume licensing activation are:

- Key Management Service (KMS)
- Active Directory-based activation (ADBA)
- Multiple Activation Key (MAK)

You can change the activation setting after you create the machine catalog.

Key Management Service (KMS)

The KMS is a lightweight service that does not require a dedicated system and can easily be co-hosted on a system that provides other services. This functionality is supported on all Citrix supported Windows versions. During image preparation, MCS does the Microsoft Windows and Microsoft Office KMS rearm. You can skip rearm by running the command `Set-Provserviceconfigurationdata`. For more information on KMS activation, see Activate using Key Management Service.

NOTE:

All machine catalogs created after running the command `Set-Provserviceconfigurationdata` have the same setting as provided in the command.

Active Directory-based activation (ADBA)

ADBA enables you to activate machines through their domain connections. Machines are immediately activated when they join the domain. These machines remain activated as long as they remain joined to the domain and in contact with it. This functionality is supported on all Citrix supported Windows versions. For more information on Active directory-based activation, see Activate using Active Directory-based activation.

Multiple Activation Key (MAK)

MAK is a way of activating volume and authenticating the Windows system with the help of the Microsoft server. You must buy the MAK key from Microsoft which is assigned with a fixed number of activation counts. Every time a Windows system is activated, the activation count reduces. There are two ways of activating the system:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Online Activation: If the Windows system that you want to activate has internet access, the system automatically activates the Windows on installing the product key. This process reduces the activation count by 1 for the corresponding MAK.
- Offline Activation: If the Windows system is not able to connect to the internet to do the online activation, MCS gets a confirmation id and an installation id from the Microsoft server to get the Windows system activated. This way of activation is useful for non-persistent machine catalogs.

NOTE:

- MCS doesn't support Microsoft Office activation using MAK.
- The minimum VDA version required is 2303.

Key requirements

- The Delivery Controller™ must have internet access.
- Create a new catalog if the new image to be updated has a different MAK Key from the original.
- Install the MAK key on the master image. See Deploy MAK Activation for the steps to install MAK Key on a Windows System.
- If you are not using image preparation:

  a. Add the registry DWORD value `Manual` under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.

  b. Set the value to `1`.

Activation Counts

To view the number of activations remaining for MAK Key or to check if a VM is consuming two or more activations, use the Volume Activation Management Tool (VAMT). See Install VAMT.

Activate the Windows system using MAK

To activate the Windows system using MAK:

1. Install the product key on the master image. This step consumes one activation count.
2. Create an MCS machine catalog.
3. If you aren't using image preparation:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

   a. Add the registry DWORD value `Manual` under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.
   b. Set the value to `1`.

   This method disables the option of online activation.

4. Add VMs to the machine catalog.
5. Power on the VMs.
6. Depending on whether it's online or offline activation, the Windows system is activated.

   - If the activation is online, the Windows system is activated after the product key is installed.
   - If the activation is offline, MCS communicates with provisioned VMs to get the activation status of the Windows system. MCS then retrieves a confirmation id and an installed id from the Microsoft server. These IDs are used to activate the Windows system.

Troubleshooting

If the provisioned VM is not activated with the installed MAK Key, run `Get-ProvVM` or `Get-ProvScheme` command on a PowerShell window.

- The `Get-ProvScheme` command: See the parameter `WindowsActivationType` associated with the MCS machine catalog from the latest master image.
- The `Get-ProvVM` command. See the parameters `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode`, and `WindowsActivationStatusError`.

You can check the error and verify the steps to resolve the issue.

Create a machine catalog using Studio

Before creating a catalog:

- Ensure that you have created a connection to the hypervisor, cloud service, other resource that hosts your machines.
- If you have created a master image to provision machines. Ensure that you have installed a VDA on that master image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

When you are using a cloud service or hypervisor to host VMs, the catalog creation wizard might contain extra pages specific to that host. For example, when using an Azure Resource Manager master image, the catalog creation wizard contains a **Storage and License Types** page. For host-specific information, see the specific articles as mentioned in Where to go next.

Launch the catalog creation wizard

1. Sign in to Citrix Cloud.
2. In the **DaaS** tile, click **Manage** to open Studio.
3. Select **Machine Catalogs** in the left pane.
4. If this is the first catalog being created, you are guided to the correct selection (such as "Set up the machines and create machine catalogs to run apps and desktops"). The catalog creation wizard opens.
5. If you already created a catalog and want to create another, follow these steps:

    a. To organize catalogs using folders, create folders under the default **Machine Catalogs** folder. For more information, see Create a catalog folder.

    b. Select the folder where you want to create the catalog, and then click **Create Machine Catalog**. The catalog creation wizard opens.

The wizard walks you through the pages described in the following sections. The pages you see may differ, depending on the selections you make, and the connection (to a host) you use. Hosts / virtualization resources lists information sources for the supported host types.

Select a machine type

Each catalog must contain machines of only one OS type. Select one of the following on the **Machine Type** page:

- **Multi-session OS:** A multi-session OS catalog provides hosted shared desktops. The machines can be running supported versions of the Windows or Linux operating systems, but the catalog cannot contain both Windows and Linux operating systems.
- **Single-session OS:** A single-session OS catalog provides VDI desktops that you can assign to different users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Remote PC Access:** A Remote PC Access catalog provides users with remote access to their physical office desktop machines. Remote PC Access does not require a VPN to provide security.

Select machine management options

NOTE:

The page **Machine Management** does not appear if you select **Remote PC Access** on the **Machine Type** page.

The **Machine Management** page indicates how machines are managed and the tool that you want to use to deploy machines.

Select one of the options to indicate how machines must be power managed:

- **Machines that are power managed (for example, virtual machines or blade PCs)**: This option is available only if you already configured a connection to a hypervisor or cloud service.
- **Machines are not power managed (for example, physical machines)**

If you select the option **Machines that are power managed (for example, virtual machines or blade PCs)**, then select a tool to create VMs:

- **Citrix Provisioning™ Technology**
  - **Citrix Machine Creation Services (MCS)** Creates a catalog of VMs provisioned and imaged using MCS. MCS copies images cloned from a master image to those VMs.
  - **Citrix Provisioning Services (PVS)** Creates a catalog of VMs provisioned using MCS and imaged using PVS. Those VMs serve as PVS target devices and the PVS server can stream a single shared disk image to them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- This option is available only for PVS sites registered with Citrix Cloud™ and is currently limited to Azure resources.
- While you create a Citrix Provisioning catalog on the **Target Device** page, you might see that in the drop-down menu to select the farm and site for the machines to be provisioned, there are farms and sites listed that no longer exist. As a workaround, you can run the PowerShell command `Unregister-HypPvsSite` to remove the farms and sites from the database. For information on the PowerShell command, see Unregister-HypPvsSite.

- **Other service or technology** A tool that manages machines already in the data center. Citrix recommends that you use Microsoft System Center Configuration Manager or another third-party application to ensure that the machines in the catalog are consistent.

NOTE:

For Linux OS machines, see Create Linux VDAs using Machine Creation Services (MCS).

Select a desktop experience

NOTE:

The options on the **Desktop Experience** page varies according to the machine type that you select on the **Machine Type** page.

- For **Multi-session OS** machines, users are assigned a random desktop each time they log in. You get the following options on the **Desktop Experience** page:
  - Save changes on the local disk of the machine hosting virtual desktops: Persistent
  - Discard all changes and clear virtual desktops when the user logs off: Non-persistent

NOTE:

For persistent multi-session machines, changes users make to the desktops will be saved and accessible to all authorized users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For single-session OS machines, you get the following options on the **Desktop Experience** page:
  - Connect to a new (random) desktop each time the users log in.
  - Connect to the same (static) desktop each time the users log in.

  You can further decide whether changes made by users will be saved or discarded after they log off.

If you select **Save changes on the local disk of the machine hosting virtual desktops: Persistent**, the Fast Copy Clone or Full Copy Clone options are available for the **Virtual machine copy** mode on the **Virtual Machines** page. Otherwise, the **Virtual machine copy** mode is unavailable.

Select an image and a machine profile

NOTE:

- This page appears only if you select **Citrix Machine Creation Services (MCS)** on the **Machine Management** page.
- The options available on this page vary according to the hypervisor or cloud service.

Follow these steps to complete the settings on the page:

1. Select an image type for the machine catalog, and then select an image. Two types of images are available:
   - **Master image**: A snapshot or VM created as the master image. It undergoes automatic image preparation at the start of catalog creation. If needed, you can add a note for the selected image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- When you are using MCS, do not run Sysprep on master images.
- If you specify a master image rather than a snapshot, the management interface creates a snapshot, but you cannot name it.
- An error message appears if you select a snapshot or VM that is not compatible with the machine management technology you selected earlier in the wizard.
- To update images within an image node, select it in the tree, and then click the **Refresh** option at the top right corner. If you don't select any image node, clicking **Refresh** updates all images in the tree. To clear a selected node in the tree, hold **CTRL** and then click the node.

- **Prepared image**: An image that has undergone image preparation, ready for direct use in VM creation. Opting for prepared images rather than master images for catalog creation ensures faster and more reliable machine catalog creation, along with streamlined image lifecycle management. If needed, add a note for the selected prepared image.

  NOTE:

  - VMs created using prepared images don’t support hibernation.
  - Currently, creating catalogs using prepared images are available only in Amazon WorkSpaces Core, Azure and VMware environments.
  - Prepared images are required for creating catalogs in Amazon WorkSpaces Core environments.

  For more information about how to create prepared images, see Image management.

2. To inherit VM settings from a machine profile, select **Use a machine profile**, and then select a VM or ARM template spec (specific to Azure) to use as the machine profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Currently, using machine profiles is restricted to Azure, Amazon WorkSpaces Core, AWS, GCP, and VMware VMs.
- A machine profile is required for creating catalogs in Amazon WorkSpaces Core environments.

3. For VMWare deployments, when creating a machine catalog using a machine profile, you must specify the folder where you want to keep the virtual machines.

To provide the virtual machine folder location, on the catalog creation wizard, go to **Virtual Machines** page, and go to **Select a folder to place the machines** section and provide the virtual machine folder location. If not specified, the system considers the folder of the selected machine profile as the default location.

1. For AWS deployments, you can select a launch template as the machine profile.
2. Select the minimum functional level for the catalog. To enable the use of the latest product features, ensure that the master image has the latest VDA version installed.

Configure the machines

NOTE:

- The title of this page depends on what you selected on the **Machine Management** page: **Machines**, **Virtual Machines**, or **Machines and Users**.
- This page does not appear if you select **Remote PC Access** on the **Machine Type** page.
- You can create an empty catalog, which means the catalog contains no machines.

- **When using MCS to create machines:**
  - Specify how many virtual machines to create. Enter **0** (zero) if you do not want to create any. Later, to create VMs for an empty catalog, you can perform **Add machines**.
  - Choose the amount of memory (in MB) each VM has.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **IMPORTANT:**
>
> Each created VM has a hard disk. Its size is set in the master image; you cannot change the hard disk size in the catalog.

- If you indicate on the **Desktop Experience** page that user changes to static desktops should be saved on a separate Personal vDisk, then specify the virtual disk size in GB and the drive letter.
- If your deployment uses more than one zone (resource location), you can select a zone for the catalog.
- If you're creating static desktop VMs, select a virtual machine copy mode. See Virtual machine copy mode.
- If you're creating random non-persistent desktop VMs, you can enable and configure the write-back cache for temporary data on machines to improve I/O performance. For more information, see Configure cache for temporary data.

- **When using other tools to provide machines:**

  Add (or import a list of) machine account names. You can change the account name for a VM after you add or import it. If you have specified static machines on the **Desktop Experience** page, you can optionally specify the user name for use with each VM you add.

  > **TIP:**
  >
  > To add users, you can browse to the users or enter a semicolon-separated list of user names manually. If the users are in Active Directory, enter the names directly. If not, enter the names in this format: `<identity provider>:<user name>`. Example: `AzureAD:username`.

  After you add or import names, you can use the **Remove** button to delete names from the list while you are still on this wizard page.

- **When using other tools (not MCS):**

  An icon and tooltip for each machine added (or imported) help identify machines that might not be eligible to add to the catalog, or be unable to register with a Cloud Connector.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual machine copy mode

The copy mode that you specify on the **Machines** page determines whether MCS creates thin (fast copy) or thick (full copy) clones from the master image. (Default = thin clones)

- Use fast copy clones for more efficient storage use and faster machine creation.
- Use full copy clones for better data recovery and migration support, with potentially reduced IOPS after the machines are created.

> **NOTE:**
>
> The Full Copy Clone approach is available only for provisioning persistent VMs on multi- or single-session OSs.

Configure cache for temporary data

When using MCS to manage random non-persistent machines in a catalog, you can enable write-back cache for machines to improve I/O performance.

Write-back cache is referred to as MCSIO. For more information, see this blog article.

PREREQUISITES

To enable write-back cache, the catalog must meet these requirements:

- Uses a connection that specifies storage for temporary data. For more information, see Connections and resources.
- VDAs must be at least version 7.9 and installed with a current MCSIO driver.

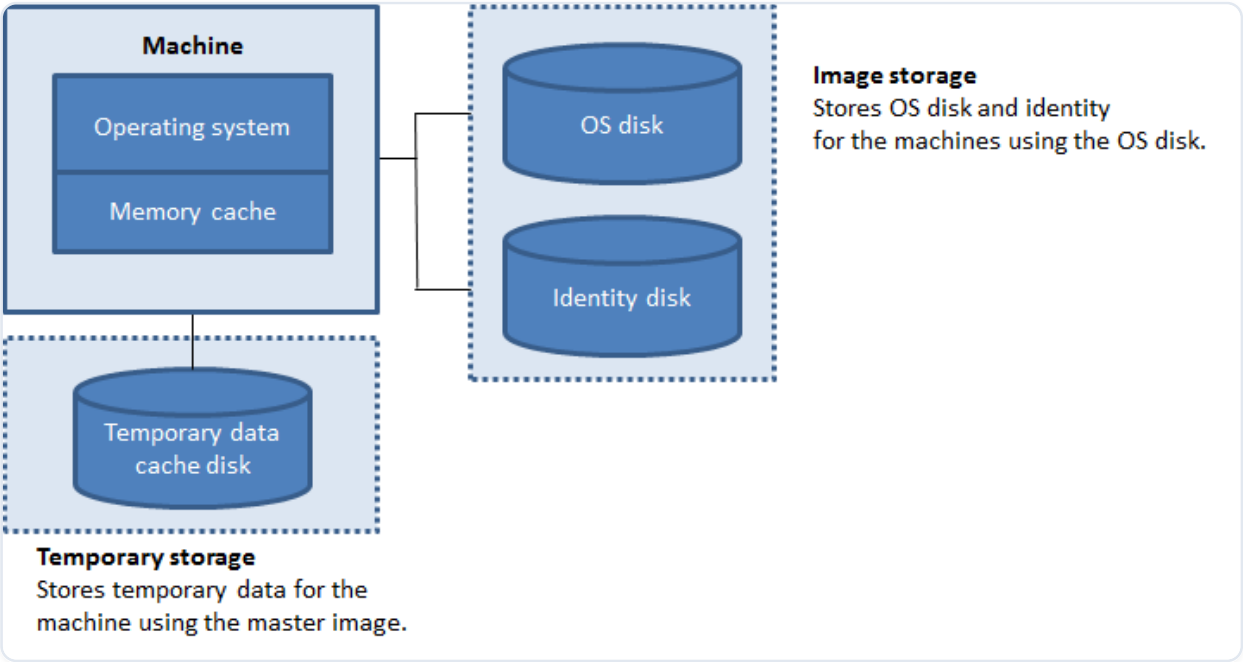
  > **NOTE:**
  >
  > You can install this driver when you install or upgrade a VDA. By default, that driver isn't installed.

- To enable drive letter assignment for disk caches, VMs must meet the following more requirements:
  - Operating System: Windows
  - VDA version: 2305 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONSIDERATIONS

- Write-back caches come in *Memory* cache and *Disk* cache. By default, their default values differ according to the connection type. Generally, the default values are sufficient for most cases; however, consider the space needed for:
  - Temporary data files created by Windows itself, including the Windows page file.
  - User profile data.
  - ShareFile data that is synced to users' sessions.
  - Data that might be created or copied by a session user or any applications users may install inside the session.



- When enabling the write-back cache for temporary data, use both a memory cache and a disk cache. Temporary data is first written to the memory cache. When the memory cache reaches the configured limit, the oldest data is moved to the disk cache. **Note:** Write-back caching using only a disk cache is no longer supported.
- The memory cache is part of the total amount of memory on each machine. Consider increasing the total amount of memory on each machine after enabling write-back cache.
- Changing **Disk cache size (GB)** from its default value can affect performance. The size must match user requirements and the load placed on the machine.

IMPORTANT:

If the disk cache runs out of space, the user's session becomes unusable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you clear the **Disk cache size** checkbox, no cache disk is created. In this case, specify a **Memory allocated to cache** value that is large enough to hold all of the temporary data. This is feasible only if large amounts of RAM are available for allocation to each VM.
- Do not enable caching if you intend to use this catalog to create AppDisks.
- You cannot change the cache values in a machine catalog after it is created.

Using CSV files to bulk add machines

If you use Studio, you can bulk add machines by using CSV files. The feature is available to all catalogs except catalogs created through MCS.

A general workflow to use CSV files to bulk add machines is as follows:

1. On the **Machines** page, select **Add CSV File**. The **Add Machines in Bulk** window appears.
2. Select **Download CSV Template**.
3. Fill out the template file.
4. Drag or browse to the file to upload it.
5. Select **Validate** to do validation checks on your import.
6. Select **Import** to complete.

For information about CSV file considerations, see Considerations when using CSV files to add machines.

You can also export machines from a catalog on the same Machines page. The exported CSV of machines can then be used as a template when adding machines in bulk. To export machines:

1. On the **Machines** page, select **Export to CSV file**. A CSV file containing a list of the machines is downloaded.
2. Open the CSV file to add or edit machines as needed. To add machines in bulk using the saved CSV file, see the previous section, Using CSV files to bulk add machines.

NOTE:

- This feature is not available for Remote PC Access catalogs.
- Export and import of machines in CSV files is only supported between catalogs of the same type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security

The **Security** page appears only if you are creating a machine catalog without assigning a machine profile in AWS virtualization environment. Use the **Security** page to configure the security groups for the VMs. This is also applicable when editing and cloning an existing machine catalog.

If you create a machine profile-based machine catalog, then the security group configurations are inherited from the machine profile and the **Security** page does not appear.

Configure NICs for the machines

The page **NICs** does not appear if you select **Remote PC Access** on the **Machine Type** page.

If you plan to use multiple NICs, associate a virtual network with each card. For example, you can assign one card to access a specific secure network, and another card to access a more commonly used network. You can also add or remove NICs from this page.

NOTE:

For VMware deployments, when creating a machine catalog using a machine profile, the catalog inherits the NIC configurations from the machine profile. In such cases, if the machine profile has multiple NICs with the same network, then Studio uses the network from the hosting unit for NIC configurations.

Add machine accounts

NOTE:

This page **Machine Accounts** appears only when you select **Remote PC Access** on the **Machine Type** page.

Add the Active Directory machine accounts or Organizational Units (OUs). Do not use a forward slash (/) in an OU name.

You can choose a previously configured power management connection or select not to use power management. If you want to use power management but a suitable connection has not been configured yet, you can create that connection later and then edit the machine catalog to update the power management settings.

You can also bulk add machines by using CSV files. A general workflow to do that is as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. On the **Machine Accounts** page, select **Add CSV File**. The **Add Machines in Bulk** window appears.
2. Select **Download CSV Template**.
3. Fill out the template file.
4. Drag or browse to the file to upload it.
5. Select **Validate** to do validation checks on your import.
6. Select **Import** to complete.

For information about CSV file considerations, see Considerations when using CSV files to add machines.

Configure identities for machines in the catalog

NOTE:

- The page **Machine Identities** appears only when you do not select **Remote PC Access** on the **Machine Type** page and select **Citrix Machine Creation Services (MCS)** on the **Machine Management** page.

Each machine in the catalog must have a unique identity. This page lets you configure identities for machines in the catalog. The machines are joined to the identity after they are provisioned. You cannot change the identity type after you create the catalog.

A general workflow to configure settings on this page is as follows:

1. Select an identity from the list.
2. Indicate whether to create accounts or use existing ones, and the location (domain) for those accounts.

You can select one of the following options:

- **On-premises Active Directory**: Machines owned by an organization and signed into with an Active Directory account that belongs to that organization. They exist on-premises.

  NOTE:

  By default, the domain where the resource (connection) resides is selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Microsoft Entra joined**: Machines owned by an organization and signed into with a Microsoft Entra account that belongs to that organization. They exist only in the cloud. For information about the requirements, limitations, and considerations, see Microsoft Entra joined.

  NOTE:

  - This option requires that the master image meets the operating system prerequisite. For more information, see the Microsoft documentation Microsoft Entra joined devices.

- **Microsoft Entra hybrid joined**. Machines owned by an organization and signed into with an Active Directory Domain Services account that belongs to that organization. They exist in the cloud and on-premises. For information about the requirements, limitations, and considerations, see Microsoft Entra hybrid joined.

  NOTE:

  - Before you can use Microsoft Entra hybrid join, make sure that your Azure environment meets the prerequisites. See Configure Microsoft Entra hybrid join.
  - This option requires that the master image meets the operating system prerequisite. For more information, see Microsoft Entra hybrid joined devices.

- **Non-domain-joined**. Machines not joined to any domain. For information about the requirements and limitations, see Non-domain-joined.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

- If you select **On-premises Active Directory** or **Microsoft Entra hybrid joined** as the identity type, each machine in the catalog must have a corresponding Active Directory computer account.
- The **Non-domain-joined** identity type requires version 1811 or later of the VDA as the minimum functional level for the catalog. To make it available, update the minimum functional level.
- The **Microsoft Entra joined** and **Microsoft Entra hybrid joined** identity types require version 2203 or later of the VDA as the minimum functional level for the catalog. To make them available, update the minimum functional level.
- A Microsoft Entra service account is mandatory when creating Microsoft Entra only or Microsoft Entra catalogs enrolled in Microsoft Intune for persistent and non-persistent VMs.

Before configuring machine identities, make sure that you have permission to create computer accounts in the OU where the machines reside. Each machine in the catalog must have a unique name. Then choose how to configure machine identities:

- If you create new machine accounts, specify the OU and the machine naming scheme. For more information, see Machine account naming scheme. When you create a catalog, an identity pool is created automatically to hold all machine identities that you defined for this catalog.
- If you use existing machine accounts, choose an existing identity pool in your environment.

NOTE:

Make sure that OU names do not use forward slashes (`/`).

When you create a catalog and select **Use existing identity pool** on the **Machine Identities** page, the service account behavior depends on the identity pool configuration:

- If the selected identity pool does not have a service account configured, selecting a stored service account on the **Domain credentials** page does not take effect. The **Add machines** operation can fail with an error indicating that the service account cannot be found. To avoid this, manually enter domain credentials on the **Domain credentials** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If the selected identity pool has a service account configured, any service account selected on the **Domain credentials** page is ignored. The **Add machines** operation always uses the service account associated with the identity pool.

If you use existing accounts, browse to the accounts or click **Import** and specify a `.csv` file containing account names. The imported file content must use the format: `[ADComputerAccount] ADcomputeraccountname.domain`

Ensure that there are enough accounts for all the machines you are adding. Studio manages those accounts. Therefore, either allow that interface to reset the passwords for all the accounts or specify the account password, which must be the same for all accounts.

For catalogs containing physical or existing machines, select or import existing accounts and assign each machine to both an Active Directory computer account and to a user account.

Machine account naming scheme

Each machine in a catalog must have a unique name. You must specify a machine account naming scheme when creating a catalog. Use wildcards (hash marks) as placeholders for sequential numbers or letters that appear in the name.

When specifying a naming scheme, consider the following:

- The maximum number of characters allowed is 15.
- The naming scheme must contain at least one wildcard character. You must put all wildcards together.
- The entire name, including wildcards, must contain at least 2 but no more than 15 characters. It must include at least one non-numeric and one # (wildcard) character.
- The name must not include spaces or any of the following characters: `,~!@'$%\^&.(){\/*?"<>|=+[];:_".`.
- The name cannot end with a hyphen (-).
- The number of characters increases with the increase in the number of machine accounts. For example, if you create 1,000 machine accounts with the scheme "veryverylong#", the last account name created (veryverylong1000) contains 16 characters that exceed the number of maximum characters allowed.

You can indicate whether the sequential values are numbers (0-9) or letters (A-Z):

- **0-9**. If selected, the specified wildcards resolve to sequential numbers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> If there is only one wildcard (#), the account names start with 1. If there are two, the account names start with 01. If there are three, the account names start with 001, and so on.

- **A-Z**. If selected, the specified wildcards resolve to sequential letters.

For example, a naming scheme of PC-Sales-## (with **0-9** selected) results in accounts named PC-Sales-01, PC-Sales-02, PC-Sales-03, and so on.

Optionally, you can specify what the account names start with.

- If you select **0-9**, accounts are named sequentially, starting with the specified numbers. Enter one or more digits, depending on how many wildcards you use in the preceding field. For example, if you use two wildcards, enter two digits or more.
- If you select **A-Z**, accounts are named sequentially, starting with the specified letters. Enter one or more letters, depending on how many wildcards you use in the preceding field. For example, if you use two wildcards, enter two letters or more.

Add domain credentials

Enter the credentials of an administrator who has permission to perform account operations. Detailed steps are as follows:

1. Click Enter credentials. The Windows Security page appears.
2. In the User name field, enter the administrator's SamName, user name, or user SID. Depending on your input:
   - If you enter a SamName, the **Domain** field populates automatically.
   - If you enter a user name or SID, you can limit the user search to a specific domain by entering the domain name or SID in the **Domain** field.
3. Click **Check name** to check whether the user name is valid or unique.
4. In the **Password** field, enter the domain password of the administrator.
5. Click **Done**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If the identity type you selected in **Machine Identities** is **Microsoft Entra hybrid joined**, the credentials you enter must have been granted the `Write userCertificate` permission.

Select a WEM configuration set for Experience Optimization

NOTE:

The page **Experience Optimization** appears only when you have a Workspace Environment Management™ (WEM) entitlement.

Improve resource allocation and enhance system performance on your machines by specifying a WEM configuration set for the machine catalog.

Required permissions

By default, creating and managing configuration sets for machine catalogs requires the **WEM Full Administrator** role, along with one of the following roles:

- **Full Access Administrator**
- **Cloud Administrator**
- **Machine Catalog Administrator**

To allow other roles to manage configuration sets, assign them both the **Manage configuration sets** permission and the **WEM Full Administrator** role.

Prerequisites

Before binding a catalog to a configuration set, ensure that your **Workspace Environment Management (WEM)** service deployment is set up. Sign in to Citrix Cloud and launch the WEM service. For more information, see Get started with Workspace Environment Management service.

If you already use WEM, verify that the **WEM agent** is installed on each VDA and connected to Citrix Cloud so that the optimization settings can take effect.

Steps

Select an **Experience Optimization** option to apply to the machine catalog:

- **Apply default settings:** Select this option to apply the default optimization settings, including automatic CPU spike protection and intelligent CPU optimization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Apply custom settings:** Select this option to create a configuration set for this machine catalog using the catalog name. After the configuration set is created, you can customize the optimization settings as needed. Alternatively, you can select an existing configuration set.

Upgrade VDA (optional)

IMPORTANT:

- To ensure a smooth upgrade, make sure that you meet the prerequisites and review known issues before upgrading VDAs to CR or LTSR CU versions. See Upgrade VDAs using Studio.
- When upgrading LTSR VDAs to LTSR Cumulative Update (CU) versions, make sure that the version of the VDA Upgrade Agents running on the VDAs is 7.36.0.7 or later. For more information, see Upgrade VDAs using Studio.

This feature applies to the following machine types:

- MCS-provisioned persistent machines. You deploy them using **Citrix Machine Creation Services** on the **Machine Management** page during catalog creation.
- Machines that are not created using MCS (for example, physical machines). You deploy them using **Other service or technology** on the **Machine Management** page during catalog creation.

For more information about the two options, see Machine management

On the **VDA Upgrade** page, select the VDA version to upgrade to. If specified, the VDAs in the catalog that have the VDA Upgrade Agent installed can upgrade to the selected version — immediately or at a scheduled time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- This feature supports upgrading only to the latest VDA. The time at which you create a VDA upgrade schedule or upgrade a VDA determines the latest version of the VDA.
- After you configure VDA upgrade settings, it might take up to 15 minutes for the **VDA Upgrade** field to reflect the latest status. To show the **VDA Upgrade** column, click the Columns to display icon in the upper right corner, select **Machine Catalog > VDA Upgrade**, and click **Save**.

Choose a VDA track that suits your deployment:

IMPORTANT:

You can switch between the CR VDA and the LTSR VDA as long as you switch from an earlier version to a later version. You cannot switch from a later version to an earlier version because that is considered a downgrade. For example, you cannot downgrade from 2212 CR to 2203 LTSR (any CU) but you can upgrade from 2112 CR to 2203 LTSR (any CU).

- **Latest CR VDA**. Current Releases (CRs) deliver the latest and most innovative app, desktop, and server virtualization features and functionality.
- **Latest LTSR VDA**. Long Term Service Releases (LTSRs) are recommended for large enterprise production environments that prefer to keep the same base version for an extended period.

After catalog creation, you can upgrade VDAs as needed. For more information, see Upgrade VDAs.

If you want to enable VDA upgrade later, you can return to this page by editing the catalog after catalog creation. For more information, see Configure VDA upgrade settings by editing a catalog.

Review the settings

On the **Summary** page, review the settings you specified. Enter a name and description for the catalog. This information appears in Studio.

When you're done, select **Finish** to start the catalog creation.

In **Machine Catalogs**, the new catalog appears with an inline progress bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To view details of the creation progress:

1. Hover the mouse over the machine catalog.
2. In the tooltip that appears, click **View details**.

   A step-by-step progress graph appears where you can see the following:

   - History of steps
   - Progress and running time of the current step
   - Remaining steps

Create an MCS machine catalog using PowerShell commands

You can also create an MCS machine catalog using PowerShell commands. For more information, see:

- SDKs and APIs
- Manage Citrix DaaS using Remote PowerShell SDKs
- New-ProvScheme

Assign a specific drive letter to an MCS I/O write-back cache disk

You can assign a specific drive letter to an MCS I/O write-back cache disk. This implementation helps you to avoid conflicts between the drive letter of any applications that you use and the drive letter of MCS I/O write-back cache disk. To do this, you can use PowerShell commands. The supported hypervisors are Azure, GCP, VMware, SCVMM, and XenServer.

NOTE:

This feature requires VDA version 2305 or later.

Limitations

- Applicable to only Windows operating system
- Applicable drive letter for write-back cache disk: `E` to `Z`
- Not applicable when Azure temporary disk is used as a write-back cache disk
- Applicable only when you create a new machine catalog

Assign a drive letter to a write-back cache disk

To assign a drive letter to a write-back cache disk:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the **PowerShell** window.
2. Run `asnp citrix*`.
3. Create an identity pool if not already created.
4. Create a provisioning scheme using the `New-ProvScheme` command with the property `WriteBackCacheDriveLetter`. For example:

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. Finish creating the catalog.

Important consideration about setting custom properties

Custom properties must be set correctly at `New-ProvScheme` and `Set-ProvScheme` in GCP and Azure environments. If you specify a non-existing custom property or properties, you get the following error message, and the commands fail to run.

`Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`

Important consideration about setting ProvScheme parameters

When you use MCS to create a catalog, you get an error if you:

- Set the following `New-ProvScheme` parameters in unsupported hypervisors when you create a machine catalog:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	SUPPORTED HYPERVISOR
`UseWriteBackCache`	VMware
	Hyper-V
	XenServer®
	Azure
	GCP
`DedicatedTenancy`	Azure
	GCP
	AWS
`TenancyType`	Azure
	GCP
	AWS
`UseFullDiskCloneProvisioning`	VMware
	Hyper-V
	XenServer

- Update the following `Set-ProvScheme` parameters after you create the machine catalog:
  - `CleanOnBoot`
  - `UseWriteBackCache`
  - `DedicatedTenancy`
  - `TenancyType`
  - `UseFullDiskCloneProvisioning`

Add SIDs while creating virtual machines

You can add the parameter `ADAccountSid` to uniquely identify the machines while creating new virtual machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To do this:

1. Create a catalog with the supported identity type.
2. Add machines to the catalog using `NewProvVM`. For example:

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

However, you cannot provision a machine with:

- An AD account that is not in the catalog identity pool
- An AD account that is not in available state

Validate configuration before creating an MCS machine catalog

You can validate configuration settings before creating an MCS machine catalog using the parameter `-validate` in `New-ProvScheme` command. After you run this PowerShell command with the parameter, you get an appropriate error message if there is an incorrect parameter used or a parameter has conflict with another parameter. You can then use the error message to resolve the issue and successfully create an MCS machine catalog using PowerShell. Currently, this feature is applicable to AWS, Azure, GCP, and VMware virtualization environments.

NOTE:

While validating, you must not create an actual MCS machine catalog. You must use the result of the command to fix the errors, and then create a successful catalog. Therefore, while running the `New-ProvScheme` command, use a fake identity pool name.

To validate the configuration, do the following steps:

1. Open a PowerShell window from the Delivery Controller host.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run `New-ProvScheme` command and use the parameter `-validate`. Provide a fake identity pool name for the command to work. For example,

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg"
-IdentityPoolName``"mptmpcatalogdemo" -InitialBatchSizeHint 1  -
MasterImageVM "XDHyp:
\HostingUnits\vSanRg\Windows19MasterImage.``vm\Citrix_XD_NonMachineProf
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
ileWin19Machines.snapshot" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vSanRg\\VM Network.network"} -ProvisioningSchemeName`
`"MachineProfileW10Machines"  -Scope @()

-VMCpuCount 2  -VM

MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-Win11-
tpm-BL-TEMPLATE.``template" -TenancyType Shared  -FunctionalLevel
"L7_20" -Validate

$result.TerminatingError | Format-List -Property *
```

Error message:

```
ErrorData    : {[[ValidationFailureCount, xxx], [InvalidMemoryValue,
The memory size provided 6143 must be a multiple of 4 MB and must be
greater than or equal to 4 MB.], [InconsistentGuestOsSetting, The
GuestOs setting - windows9_64Guest of the selected machine profile does
not match with the setting - windows2019srv_64Guest of master image.
Please select a machine profile that matches the GuestOs setting of the
master image.], [InconsistentVtpmSetting, The vTPM setting of the
selected machine profile does not match with the selected master image.
Please select a machine profile that matches the vTPM setting of the
master image.], [InconsistentFirmwareSetting, The firmware setting -
efi of the selected machine profile does not match with the setting -
bios of master image. Please select a machine profile that matches the
firmware setting of the master image ErrorId      : ValidationFailure

ErrorMessage : ValidationFailure

Operation    : ValidatingInputs
```

4. After validating the configuration setting, you can create an MCS machine catalog with a real identity pool name and correct parameters.

Onboard VMs to Azure Arc

Azure Arc enables organizations to manage resources such as VMs hosted anywhere as if they are running in Azure. With Azure Arc, you can use Azure services such as Azure Monitor for comprehensive visibility and proactive management of the resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To onboard VMs to Azure Arc, create an MCS machine catalog using the `New-ProvScheme` command. You can also update an existing catalog using the `Set-ProvScheme` command. Only the new VMs added to the catalog are onboarded to Azure Arc.

Currently, this feature is applicable to all Citrix on-premises hypervisors VMware, Nutanix and SCVMM.

Prerequisites

Consider the following before enabling Azure Arc onboarding on MCS catalog:

- Azure Resource Group with:
  - `Allows` accounts to read, create, and delete Arc servers.
  - `Allows` accounts to manage VM extensions, licenses, and private link scopes.
  - `Azure Connected Machine Resource Administrator` role assigned to the service principal at the resource group scope.

See Assign Azure roles using the Azure portal.

- Master image with
  - VDA: Later than 2311, excluding 2411.

    NOTE:

    Azure Arc Onboarding is not supported in Citrix Virtual Apps and Desktops 2411.

  - AzureConnectedMachineAgent agent installed. You might download the MSI from under Windows or Linux sections of Microsoft's documentation.

Steps to onboard VM to Azure Arc

1. Setup a service account with `AzureArcResourceManagement` capability.

   The service account is used for authentication or authorization by storing credentials to access identity providers like Microsoft Entra ID. Each service account is tied to a single identity provider.

   To create a new service account to access Azure AD with `AzureArcResourceManagement capability`, run:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-AcctServiceAccount -IdentityProviderType “AzureAD”
-IdentityProviderIdentifier “tenant-id” -AccountId “application-id”
-AccountSecret “application-secret” -Capabilities
“AzureArcResourceManagement”
```

The `application-id` must be of the same service principal that was assigned the Azure Connected Machine Resource Administrator role.

2. Assign the service account to the identity pool. For example:

```
Set-AcctIdentityPool -IdentityPoolUid “idn-pool-uid” -ServiceAccountUid
“service-account-uid”
```

3. Create or update an MCS catalog with the following Arc parameters:

   - `EnableAzureArcOnboarding`: Indicates whether Arc Onboarding needs to be enabled on the catalog.
   - `AzureArcSubscriptionId`: Indicates the Azure subscription where the Arc-connected VMs are created.
   - `AzureArcRegion`: Indicates the Azure region where the Arc-connected VMs are created.
   - `AzureArcResourceGroup`: Indicates the Azure resource group where the Arc-connected VMs are created. See Prerequisites for information on Azure Arc Resource Group.

   Example: To enable Azure Arc Onboarding for a new catalog:

```
`New-ProvScheme -ProvisioningSchemeName "demo" -MasterImageVM "XDHyp:
\HostingUnits\hosting-unit\masterVMName.vm\masterSnapshotName.snapshot"
-HostingUnitName “hosting-unit” -IdentityPoolName “identity-pool”`



-EnableAzureArcOnboarding -AzureArcSubscriptionId “azure-sub”
-AzureArcResourceGroup “azure-resourcegroup” - AzureArcRegion “azure-
region”
```

   Example: To enable Azure Arc Onboarding for an existing catalog:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding
$true -AzureArcSubscriptionId “azure-sub” -AzureArcResourceGroup
“azure-resourcegroup” - AzureArcRegion “azure-region”
```

Example: To disable Azure Arc Onboarding for an existing catalog:

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding
$false:
```

4. Add new machines to the catalog to onboard Arc.
5. After you power-on the VM, you must see the VM in the Azure portal under **AzureArcResourceGroup** as a connected machine.

Considerations

- Arc onboarding is currently supported for only new VMs. So, if you update an existing catalog using `Set-ProvScheme`, then only newly added VMs are onboarded to Arc when first powered on.
- The Arc Custom Properties are still supported for existing catalogs for backward compatibility. However, if you run `New-ProvScheme` with Arc CustomProperties such as `EnableAzureArcOnboarding`, then catalog creation fails.
- You must add all the parameters in `New-ProvScheme` and `Set-ProvScheme` if you configure `EnableAzureArcOnboarding` as `true`.

Troubleshooting

When creating SCVMM catalog using `New-ProvScheme`, you might get the following error:

```
Master Image/Machine Profile's VM's device id is different than the
NetworkMapping's device id '0'. Please provide a device id that matches
the master image/machine profile.
```

In that case, make sure you explicitly specify the `DeviceId` in `NetworkMapping` parameter of `New-ProvScheme`. For example:

```
New-ProvScheme -ProvisioningSchemeType "MCS" -InitialBatchSizeHint 1
-HostingUnitName $HostingUnitName `

            -IdentityPoolName $CatalogName -MasterImageVM $MasterImage
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-ProvisioningSchemeName $CatalogName `

            -VMCpuCount 2 -VMMemoryMB 4096  -EnableAzureArcOnboarding `

            -AzureArcSubscriptionId $AzureArcSubscription -AzureArcRegion
$AzureArcRegion `

            -AzureArcResourceGroup $AzureArcResourceGroup

            -NetworkMapping @{"FDDxxxxxx-xxxx-4xxx-9EBC-3xxxxxxxx"="XDHyp:
\HostingUnits\<hosting unit name>\abc.network"}
```

Follow-Me Tagging

Follow-Me Tagging enables tracking of individual end-user VM usage by applying hypervisor-level tags. These tags, labeled with the specific user and/or organization (using `citrix-user-upn` as the key and the User Principal Name (UPN) as the value), are automatically added by Citrix when a user is assigned to a VM and removed when the user is unassigned.

Advantages

This feature offers several advantages:

- **IT chargeback**: Facilitates filtering resource usage (Azure: NICs, OS, ID, WBC, Data disks, and VMs) (AWS EC2: EC2 instance, EBS volumes (OS, ID, WBC, and Data disks), and NICs) by tags, allowing for accurate chargeback to individual users or business units.

  NOTE:

  - For AWS EC2, activate the `citrix-user-upn` tag key as a cost allocation tag to make it appear in your billing report. See Activating AWS-generated tags cost allocation tags.
  - For Azure, you need not activate the `citrix-user-upn` tag to filter cost analysis reports by user to view detailed spending, that includes, monthly total spend, costs per individual resource, daily cost trends, costs by service, and detailed billing records.

- **Efficient user management**: Automates the removal of tags from resources when end-users are unassigned (for example, employment changes like termination or reorganization).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Enhanced security monitoring**: Helps identify VMs assigned to specific end-users for targeted security scans.

Applicability

Currently, follow-me tagging is applicable to:

- AWS EC2 and Azure environments
- Statically assigned machines running single-session OS
- Persistent and Non-persistent catalogs
- All supported machine identity joined catalogs
- Only MCS provisioned VMs
- Managed disks (for Azure) only

Limitations

- A brief synchronization period exists between end-user assignment and the appearance of the corresponding tag on the hypervisor's machine.
- MCS doesn’t retry tagging operations if the tagging operation fails due to issues like insufficient tagging permissions, hypervisor failures, or unavailable Cloud Connectors. Instead, MCS issues a warning on the provisioning scheme. This warning can be accessed using the PowerShell command `Get-ProvOperationEvent`.
- Tag operations are initiated exclusively when a catalog's tagging is enabled or disabled, or when a user is assigned to a VM.
- If you manually remove the follow-me tag from the NIC, the tag doesn’t apply to any newly created resources on the next power on.

Important considerations

Consider the following when using follow-me tagging in AWS EC2 environments:

- AWS specific limitations: See Tagging limitations for tagging limitations.
- Activate the tag for cost allocation. See Activating AWS-generated tags cost allocation tags.

Consider the following when using follow-me tagging in Azure environment:

- Azure specific limitations
- You can add only 50 tags per resource.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure follow-me tagging

You can configure the follow-me tagging using Studio and PowerShell.

Use Studio

In the Machine Catalog Setup wizard:

1. On the **Operating System** page, select **Single-session OS.**
2. On the **Machine Management** page:
   - Select **Machines that are power managed (for example, virtual machines or blade PCs).**
   - Select to deploy machines using **Citrix provisioning technology Citrix Machine Creation Services (MCS)**.
3. Complete the settings on the following pages.
4. On the **Virtual Machines** page, select **Apply follow-me tagging**.
5. Complete the catalog creation process.
6. To verify that the feature is enabled for the catalog, navigate to the **Details** page for the created catalog. The **Follow-me tagging** capability under **Machine** must show as **Enabled**.
7. From the left-pane, select **Delivery groups**, click **Create Delivery Group**. Add the created catalog to a delivery group and assign one or more users to the delivery group.

MCS automatically tags a VM in the catalog with the first user who logs on to the machine. Alternatively, users can be manually assigned to a machine instead of relying on the first logon.

You can also edit an existing catalog to configure the follow-me tagging.

1. Select the catalog you want to modify and click **Edit Machine Catalog**.
2. Navigate to the **Virtual Machines** section and select **Apply Follow-me Tagging**.
3. Click **Apply** and then **Save** to enable the feature for the existing catalog. New and existing VMs in this catalog are now tagged at the hypervisor when end users are assigned.

Use PowerShell

To configure follow-me tagging using PowerShell, use the `-HypervisorVMTagging` parameter with the `Set-BrokerCatalog` cmdlet and set it to `$true`.

Example script to enable tagging:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-BrokerCatalog -Name 'CatalogName' -HypervisorVMTagging $true
```

Example Script to check tagging status for a catalog:

```
Get-BrokerCatalog -Name "SS-S-P-Cat" | Select Name, SessionSupport,
AllocationType, ProvisioningType, HypervisorVMTagging
```

Check the value of `HypervisorVMTagging`. If follow-me tagging is enabled for the catalog, then the value of `HypervisorVMTagging` is `True`.

After enabling the follow-me tagging for the catalog, add the created catalog to a delivery group and assign one or more users to the delivery group.

Use follow-me tagging

After you enable follow-me tagging for a machine catalog and users are assigned to the VMs within that catalog, MCS automatically applies a hypervisor-level tag to the virtual machines. This tag is in the format `citrix-user-upn:<User Principal Name (UPN)>`. Use this tag within your hypervisor's billing and management console to track resource usage by specific end users.

To analyze costs for resources with specific tags in Azure:

1. Go to the **Cost Analysis** page on Azure Portal.
2. Add the **Tag** filter.
3. Use `citrix-user-upn` as the key.
4. Select one or more desired UPNs to track resource costs.
5. View the actual costs accumulated for the tagged resources.

Use the tag filtering with `citrix-user-upn` to:

- See a user's monthly total spending (Accumulated costs view).
- View all resources owned by a specific user and their costs (Cost by resources view).
- Detect unexpected increases in daily costs per user (Daily costs view).
- Identify which services a user is spending on, such as VMs or Storage (Cost by service view).
- Build detailed user-level billing records by filtering raw billing line items (Invoice details view).

To analyze costs for resources with cost allocation tags in AWS:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Activate the cost allocation tags (It takes up to 24 hours for it to get activated and to be visible in the Billing Report). Activate the cost allocation tags through EC2 billing console or thorough AWS cost explorer API, `UpdateCostAllocationTagsStatus`.
2. Add the cost allocation Tag Key and some value to the AWS resources.

Using these tags, generate the billing reports to view the cost incurred by resources as per the cost allocation tag key and specific values. You can view the report on monthly, daily, and hourly granularity.

When a user is unassigned from a machine, MCS automatically removes the corresponding tag from that VM.

Troubleshooting

- **Problem**: Tags are not appearing on the hypervisor after user assignment.
- **Cause**: There might be a sync-up delay, or MCS failed to perform tagging due to permissions issues, hypervisor failure, or unavailable Cloud Connectors.
- **Solution**:
  - Allow a few minutes for the tag to appear.
  - If the issue persists, check for warnings on the provisioning scheme using the PowerShell cmdlet `Get-ProvOperationEvent` to identify any errors encountered during tagging. Ensure that Citrix has the necessary tagging permissions on the hypervisor.
  - Check the tagging status. Run `Get-ProvVM` and check the `CustomMachineData` for the Boolean `IsFollowMeTagged`.

Image replication of additional storage for supported on-premises hypervisors

This feature enables efficient replication and management of image version specification instances across multiple storage locations supported by on-premises hypervisors.

Use cases

- You can replicate image versions to new or superseded storage locations, allowing virtual machines to be provisioned in additional locations either during or after the image preparation process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When a new image version is created and additional storage locations are specified, the prepared image version specification is automatically replicated to those designated storage locations.
- If there is a need to use an existing image version with a superseded or newly added storage locations, you can add an image version instance to replicate to the new storage location.
- When a hosting unit is added to an existing image version, along with additional storage, the prepared image version spec instance will be replicated to the specified additional storages within the target hosting unit.

PowerShell commands

- Add a new image instance that replicates a prepared image version spec to the specified storage location.

```
Add-ProvImageVersionSpecInstance -ImageVersionSpecUid <
ImageVersionSpecUid > -StorageIds "<StorageId1,StorageId2>"
-RunAsynchronously
```

- Remove an existing image version spec instance replica and not used by any existing VMs.

```
Remove-ProvImageVersionSpecInstance -ImageVersionSpecUid <
ImageVersionSpecUid >  -ImageInstanceUid < ImageInstanceUid >
-RunAsynchronously
```

- Get a list of image version specs instances.

```
Get-ProvImageVersionSpecInstance -ImageVersionSpecUid  <
ImageVersionSpecUid >
```

Where to go next

For information on creating specific hypervisor catalogs, see:

- Create an AWS catalog
- Create a Google Cloud Platform catalog
- Create a Microsoft Azure catalog
- Create a Microsoft System Center Virtual Machine Manager catalog
- Create a Nutanix catalog

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Create a VMware catalog
- Create a XenServer catalog

If this is the first catalog created, you are guided to create a delivery group.

To review the entire configuration process, see Plan and build a deployment.

You can create a Citrix Provisioning catalog using Studio and PowerShell. This implementation provides you the following advantages:

- A single unified console to manage both MCS and Citrix Provisioning catalogs.
- Have new features for Citrix Provisioning catalogs, such as, identity management solution, on-demand provisioning and so on.

Currently, this feature is available only for Azure and VMware workloads. However, in VMware and XenServer environments, you can currently create the catalogs using only PowerShell commands. For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

More information

- Citrix Virtual Apps and Desktops Image Management
- Create and manage connections and resources
- Identity pools of different machine identity join types
- Manage machine catalogs

Create a catalog of Amazon WorkSpaces Core Managed Instances

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Amazon WorkSpaces Core Managed Instances.

NOTE:

Currently, creation of catalogs of both persistent and non-persistent VMs (`CleanOnBoot` property is `True` or `False`) is supported.

Prerequistes

Before creating a catalog of Amazon WorkSpaces Core Managed Instances, you need to finish creating:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. A connection to Amazon WorkSpaces Core Managed Instances. See Connection to Amazon WorkSpaces Core Managed Instances
2. A prepared image. See Create a prepared image for Amazon WorkSpaces Core Managed Instances.

Network setting during image preparation

During image preparation, a preparation virtual machine (VM) is created based on the original VM. This preparation VM is disconnected from the network. To disconnect the network from the preparation VM, a network security group is created to deny all inbound and outbound traffic. This network security group persists and is reused. The network security group's name is `Citrix.XenDesktop.IsolationGroup-GUID`, where GUID is randomly generated.

A machine profile-based machine catalog

You can use a machine profile to capture the hardware properties from an EC2 instance (VM) or launch template version and apply them to the provisioned machines. Properties that are captured can include, for example, tenancy type, instance type, security groups, network mappings, EBS volume properties, EBS optimization, CPU options, hibernation capability, and other supported AWS configurations.

You can use an AWS EC2 Instance (VM) or AWS Launch Template version as the machine profile input.

NOTE:

- EBS volume properties are derived only from a machine profile.
- The Instance Metadata Service (IMDS) V2 is only supported and not IMDS V1. For information, see How Instance Metadata Service Version 2 works.

AWS tenancy

AWS provides the following tenancy options: shared tenancy (the default type) and dedicated tenancy. Shared tenancy means that multiple Amazon WorkSpaces Core instances from different customers might reside on the same piece of physical hardware. Dedicated tenancy means that your Amazon WorkSpaces Core instances run only on hardware with other instances that you have deployed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The dedicated instances are only supported (dedicated hosts are currently not supported). Other customers do not use the same piece of hardware.

Tenancy type is captured from machine profile

When you use MCS to create a catalog to provision machines in AWS, the tenancy type is captured from the machine profile.

- **Shared hardware**: This setting is suitable for most deployments. Multiple customers share pieces of hardware even though they do not interact with each other. Using shared hardware is the least expensive option for running your Amazon EC2 instances.
- **Dedicated instance**: This setting is more suitable for deployments with specific security or compliance requirements. With a dedicated instance, you still enjoy the benefits of having a host separate from other AWS customers but you do not pay for the entire host. You do not need to worry about the capacity of the host but you are charged at a higher rate for the instances. Additionally, Dedicated Instances provide limited support for Bring Your Own License (BYOL).

Flexible billing

Amazon WorkSpaces Core Managed Instances supports two billing modes:

BILLING MODE	DESCRIPTION
Monthly	Fixed, monthly flat-rate billing. Ideal for persistent desktops and predictable workloads.
Hourly	Pay-as-you-go billing. This is the AWS default configuration if no billing mode is explicitly specified.

These options provide flexibility for managing compute costs based on your workload's persistence and usage patterns.

This feature requires the use of the Amazon WorkSpaces billing service. By default, MCS uses this service to provision and manage instances, letting you benefit from more competitive flat-rate pricing for persistent workloads.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites and considerations

- AWS account configuration: Your AWS account must be configured to use the WorkSpaces billing service. While AWS accounts are switched by default, some customers may request AWS to remain on the legacy EC2 billing service for using WorkSpaces Core Managed Instances.

  NOTE:

  If your account is on the legacy EC2 billing service, the **Monthly** billing option is not available.

- Host connection: Flexible billing is only applicable to Amazon WorkSpaces Core host connections. It is not supported for standard AWS EC2 host connections.
- Spot instances: Spot instances are not supported with the WorkSpaces billing service.
- Mixed billing: An AWS account must use either WorkSpaces billing or EC2 billing for core managed instances. A mix of both within a single account is not supported.
- Compatibility: Only specific instance types, platform types (OS), and tenancy types are compatible with certain billing modes. MCS performs a preflight check to ensure your selections (Service Offering, Machine Profile, and Prepared Image) match the chosen billing mode.

See Create a machine catalog with a specific billing mode.

Create a catalog

A prepared image and a machine profile is required for creating catalogs of Amazon WorkSpaces Core Managed Instances. You can use an AWS VM Instance or AWS Launch Template version as the machine profile input.

You can create a catalog using:

- Studio
- PowerShell

Create a catalog using Studio

Create a machine catalog from the Images node

Use the **Create catalog** option in the **Images** node to create a catalog using the image version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alternatively, you can select the version when creating a catalog in the **Machine Catalogs** node, linking to the prepared image option in the catalog creation workflow. See Create a machine catalog from the Machine Catalogs node.

To create an MCS machine catalog from the **Images** node, do the following:

1. Select an image version and click **Create catalog**. Click **Next** on the **Introduction** page.
2. On the **Machine Management** and **Image** pages, the settings are pre-selected based on the selected image version. On the Image page, enter a note for the selected prepared image.
3. Complete the settings on the following pages.
4. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.
5. Go to the **Machine Catalogs** node to see the created machine catalog.

Create a machine catalog from the Machine Catalogs node

To create an MCS machine catalog from the Machine Catalogs node, do the following:

1. Click **Machine Catalogs** on the left navigation pane.
2. Click **Create Machine Catalog**. The **Machine Catalog Setup** page appears.
3. On the **Machine Type** page, select a machine type for the catalog, for example, **Multi-session OS**.
4. On the **Machine Management** page, select the following settings:
    a. Select **Machines that are power managed (for example, virtual machines or blade PCs)**.
    b. Select **Citrix provisioning technology**. Then, select **Citrix Machine Creation Services™**.
    c. In the **Resources** field, select the resources (Availability Zone or Local Zone) that you configured while creating the host connection and click **Next**.
5. On the **Desktop experience** page, select either random or static desktop that you want users to have when they log in. If a static desktop is selected, further specify whether you want to save changes that the user makes on the local disk (persistent or non-persistent).
6. On the **Image** page, click **Select an image** to select a prepared image for the machine catalog. Select the prepared version that you created. Click the image version name. To view more details about the selected image version, click the version number, which is underlined. Click **Done**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The machine profile associated with the prepared image appears and its hardware properties (for example, instance type, tenancy type, network mappings, security groups, volume properties) are used to create machines in the catalogs. To change the machine profile source to another VM or launch template version click the edit button.

7. On the **Virtual Machines** page:
    a. Enter the number of VMs for the catalog.
    b. The default machine specification is displayed, which is based on the machine profile. To change it, select the edit icon and select a machine specification.
8. On the **NICs** page, select the NICs (or ENIs) for the VMs.
9. On the **Machine Identities** page, configure the machine identity type for the machines in the catalog:
    a. To configure **domain-joined machines (on-premises Active Directory or Microsoft Entra hybrid joined)**, select the domain and create new AD accounts for the VMs to be created in this machine catalog. The provisioned VMs are joined to the domain selected. To provision **non-domain joined machines**, select the non-domain join option.
    b. Specify the account naming scheme for the new accounts to be created for the VMs.
10. On the **Domain credentials** page, click **Enter credentials** to provide the credentials for the selected domain. Enter admin-level username and password when prompted. You can also use a service account if you have domain credentials already saved previously by following our product docs.
11. Click through the remaining pages until the **Summary** page. Enter a name for the machine catalog and select **Finish** to create the machine catalog.

Limitations on creating a machine catalog in an AWS local zone

- Certain local zones only support certain hardware configurations (for example, Perth local zone does not support GP3 volumes, only GP2).
- Since only gp2 is universally supported across all local zones, and not all support gp3, ID disk creation defaults to using gp2 volume type.
- You must select a machine profile with hardware specifications that are supported in the desired local zone.
- Prepared image AMIs snapshots and ID disk snapshots defaults to being placed in the region, rather than the local zone (due to AWS limitations regarding visibility into EBS snapshot support in local zones).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Only local zones supporting full EC2 and EBS services are supported zones.

Create a catalog using PowerShell

Create a catalog using a prepared image version spec and machine profile

- Create an MCS non-persistent machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$true] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

- Create an MCS persistent machine catalog from the prepared image version spec using the `New-ProvScheme` command. For example,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$false] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

Example of the complete set of Powershell commands to create a catalog:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "wsccatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "domainname"
-IdentityPoolName "wsccatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "aws##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName wsccatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-HostingUnitName wsc -IdentityPoolName wsccatalog -CleanOnBoot -Scope @()
-SecurityGroup @() -MachineProfile 'XdHyp:\HostingUnits\cvad-test-
scalestress\us-east-1a.availabilityzone\machine-profile-instance i
(i-0xxxxxxxx).vm' -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName wsccatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Update the machine profile

To update the machine profile on a catalog that was initially provisioned with a machine profile, do the following. You can also change the tenancy type and hibernation capability of the machine profile source while editing an MCS machine catalog.

1. Run `Set-ProvScheme` command. For example,

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

Create a machine catalog with a specific billing mode

You can specify the billing mode while creating a machine catalog using only PowerShell currently.

USE POWERSHELL

To specify the billing mode through PowerShell, use the `CustomProperties` parameter in the `New-ProvScheme` command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$custprop = "BillingMode,Monthly"



New-ProvScheme -ProvisioningSchemeName "MyCatalog" `

-ImageVersionSpecUid $ImageVersionSpecUid `

-HostingUnitName "wsc-unit" `

-IdentityPoolName "MyIdentityPool" `

-MachineProfile "XdHyp:\HostingUnits\wsc-unit\machine-profile
lt-123.launchtemplate\lt-123 (1).launchtemplateversion" `

-CustomProperties $custprop `

-CleanOnBoot
```

NOTE:

If the `BillingMode` property is omitted, the catalog defaults to `Hourly`.

Change the billing mode of an existing catalog

You can convert an existing catalog from `Monthly` to `Hourly`, or vice versa. This change can apply to both new and existing VMs in the catalog.

IMPORTANT CONSIDERATIONS FOR UPDATES

- Service window: Existing VMs must undergo a service window or power cycle to apply the billing change.
- Validation: MCS validates that the existing instance types and platforms are compatible with the new billing mode before applying the change.

UPDATE USING POWERSHELL

- To update the billing mode of only new VMs added to a catalog, update the billing mode custom property of the provisioning scheme:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$custprop = "BillingMode,Hourly"



Set-ProvScheme -ProvisioningSchemeName "MyCatalog" -CustomProperties
$custprop
```

- To update the billing mode of new and existing VMs in a catalog, create a new provisioning scheme version with the updated custom property, and apply the new version to all VMs:

```
$custprop = "BillingMode,Hourly"



New-ProvSchemeVersion -ProvisioningSchemeName "MyCatalog"
-CustomProperties $custprop



New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 2 `

-StartsNow -AllVMs `

-MaxDurationInMinutes 100 `

-ProvisioningSchemeName "MyCatalog"
```

Monitor billing information

You can verify the billing mode for catalogs and individual virtual machines.

Run the following PowerShell commands to check your account's billing eligibility:

- Returns `BillingMode` as part of CustomProperties

```
Get-ProvScheme –ProvisioningSchemeName “"MyCatalog" "  | Select
 ProvisioningSchemeName,  CustomProperties
```

- Returns `BillingMode` as part of VMInfo

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-ProvVMDetails –ProvisioningSchemeName “"MyCatalog" "  | Select-
Object  -ExpandProperty VMInfo
```

Troubleshooting and validation

MCS includes preflight checks to prevent incompatible configurations. You may encounter the following errors during catalog creation or editing:

- **NoInstanceConfigFoundForBillingMode**: Occurs if the selected Service Offering (instance type), Tenancy, and Platform Type are not supported for the chosen billing mode.
- **Spot Instance Not Supported**: If you attempt to use Spot instances with a WorkSpaces host connection, validation fails.
- **EC2 billing restriction**: If your AWS account is on the legacy EC2 billing model, attempting to set a Monthly billing mode results in a validation error.

Create a catalog with launch template version using PowerShell

You can create an MCS machine catalog with a launch template version as a machine profile input. You can also update the input of a machine profile catalog from a VM to a launch template version and from a launch template version to a VM.

On the AWS EC2 console, you can provide the instance configuration information of a launch template along with version number. When you specify the launch template version as a machine profile input while creating or updating a machine catalog, the properties from that version of the launch template are copied to the provisioned VDA VMs.

The following properties can be provided using machine profile input or explicitly as parameters in `New-ProvScheme` or `Set-ProvScheme`commands. If they are provided in `New-ProvScheme` or `Set-ProvScheme` commands, they take precedence over the machine profile values of these properties.

- Service Offering
- Networks

NOTE:

If service offering is not provided in the machine profile launch template or as a parameter in the `New-ProvScheme` command, you get an appropriate error.

To create a catalog using launch template version as a machine profile input:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Get the list of launch template versions of a launch template. For example:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. Create an identity pool if not created. For example:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. Create a provisioning scheme with a launch template version as a machine profile input. For example:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-ImageVersionSpecUid ‘24dfb047-e867-527g-896c-25664xxxxx1t’ `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. Register a provisioning scheme as a broker catalog. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. Complete creating the catalog.

Update the machine profile source

You can also update the input of a machine profile catalog from a VM to a launch template version and from a launch template version to a VM. For example:

- To update the input of a machine profile catalog from a VM to a launch template version:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- To update the input of a machine profile catalog from a launch template version to a VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

MCSIO enabled catalog

MCS Storage Optimization (MCSIO) improves the performance of the VM by caching disk operations in either memory or on a small, high-speed disk. You can create an MCSIO enabled non-persistent catalog using PowerShell commands. To create such a catalog, you must install the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MCSIO driver while installing or upgrading the VDA during the preparation of the AMI instance. By default, that driver is not installed.

After an MCSIO AMI is prepared (when installing the VDA, select the option to include the MCSIO driver in the installation), you can create an MCSIO enabled non-persistent catalog.

NOTE:

The option to configure MCSIO with only disk cache (without memory cache) using Studio has been removed across all hypervisors and cloud service environments.

Create an MCSIO enabled catalog

The four parameters added to the New-ProvScheme PowerShell command are:

- `UseWriteBackCache`: Turns on caching (write-back cache) for the given provisioning scheme
- `WriteBackCacheDiskSize`: Specifies the size in GB of the temporary disk used for caching
- `WriteBackCacheMemorySize`: Specifies how much memory in MB to use for caching. This is an optional parameter.

NOTE:

- The value of `WriteBackCacheDiskSize` must be more than zero because at least 1 GB of cache disk storage is required. The cache disk size must not be bigger than the OS disk size.
- The value of `WriteBackCacheMemorySize` must be non-zero and less than the machine catalog memory size.

The custom properties that affect MCSIO are:

- `WBCDiskStorageType`: Defines the volume type, which is used for the temporary disk in Amazon WorkSpaces Core Managed Instances. This parameter takes a string argument in the format `volume-type[:iops][:throughput]`. The following are the volume types:
  - gp2: Do not use iops and throughput parameters for this volume type
  - gp3: Use iops and throughput parameters for this volume type
  - io1: Use only iops parameter for this volume type
  - io2: Use only iops parameter for this volume type

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The default volume type is **gp2**.

- `PersistWBC`: Controls whether to keep or discard the cache disk whenever the Amazon WorkSpaces Core Managed Instances is powered off. If set to `true`, the cache disk is kept. If set to `false` (the default), the cache disk is only created and kept while the AMI instance is powered on.
- `PersistOSDisk`: Controls whether to keep or discard the OS disk whenever the Amazon WorkSpaces Core Managed Instances is powered off. If set to `true`, the OS disk is kept. If set to `false` (the default), the OS disk is only created and kept while the AMI instance is powered on.

Perform the following steps in the PowerShell window to create an MCSIO enabled non-persistent catalog:

1. Open the PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create a broker catalog and an identity pool.
4. Create the provisioning scheme. For example:

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'



$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. Add VMs to the catalog.

Improve boot performance with MCSIO

You can improve the boot performance of VMs if you enable MCSIO and set `PersistWBC` and `PersistOSDisk` custom properties as `true`. With such a setting, VMs can boot faster because they do not need to initialize a new cache disk or to recreate a root disk from their template.

Encrypt OS and ID disks

You can create a catalog of VMs with AWS KMS keys (Customer managed key and AWS managed key) that can be used to encrypt OS disk and Identity Disk (ID).

- AWS managed keys are automatically rotated every year.
- Customer managed keys are optional for automatic rotation and can be managed manually.

You can see the following AWS documents for more information on KMS keys:

- AWS KMS concepts
- How automatic key rotation works

For encryption of OS and ID disks, configure one of the following:

- Use a prepared image that is encrypted (for example, an AMI created from an instance or snapshot that contains an EBS root volume encrypted with KMS key)
- Use a machine profile source (VM or launch template) that contains an encrypted EBS root volume.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations

Consider the following limitations:

- MCS currently supports only one disk on prepared image AMI.
- You cannot directly encrypt existing unencrypted EBS volumes or snapshots, or modify the KMS key of an existing encrypted volume. To do that, you must:

  a. Create a new snapshot of that volume.

  b. Create a new volume from that snapshot

  c. Encrypt the new volume.

See the following AWS documents:

- Encrypt unencrypted resources
- Limitations of automatic or default encryption of EBS volumes: Automatically encrypt existing and new Amazon EBS volumes.

Create a catalog with disk encryption

You can create an MCS machine catalog with disk encryption using:

- Prepared image (created using image management from master image that has encrypted disk)
- Machine profile

Considerations while using machine profile input are:

- The KMS key of the machine profile input takes precedence over the prepared image's KMS key.
- If no machine profile input is provided, then the KMS key of the prepared image AMI is used to encrypt the disks of catalog VMs.
- If the machine profile has Block Device Mappings present, then the block devices present in the prepared image template (AMI) and the machine profile must match. For example, if AMI has a device defined on `/dev/sda1`, then the Machine Profile must also have a device defined on `/dev/sda1`.
- If there is no key in the machine profile source and the prepared image is unencrypted, then disks of catalog VMs are not encrypted.
- When the prepared image is encrypted, a machine profile source VM or launch template must have an encrypted root volume to be considered a valid input.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Modify an existing catalog

You can modify an existing catalog using the `Set-ProvScheme` PowerShell command to have:

- A machine profile input with a volume containing a new KMS key.
- A prepared image created from the master image with encrypted AMI using image management.

Important considerations:

- The volumes of new VMs added to the catalog are encrypted with the new KMS key.
- To update the encryption settings when there is an existing machine profile, run `Set-ProvScheme` with a new machine profile.
- You cannot modify an existing catalog from having encrypted volumes to unencrypted volumes. You cannot do an image update from an encrypted prepared image AMI to an unencrypted prepared image AMI.

Enable NitroTPM and UEFI secure boot for VM instances

When creating a catalog, you can now select a prepared image (AMI) with NitroTPM and/or UEFI secure boot enabled. Accordingly, the provisioned VMs in the catalog are also enabled with NitroTPM and/or UEFI secure boot. This implementation ensures that the VMs are secured and trusted. For more information on NitroTPM and UEFI Secure Boot, see the Amazon documentation.

Limitations

- You can use both NitroTPM and Secure Boot currently in all AWS Regions (including the AWS GovCloud (US) Regions) except China.
- You cannot enable NitroTPM and UEFI secure boot on existing catalogs. If you want a catalog with NitroTPM and UEFI secure boot enabled, create a new catalog.

Key steps

1. Set up your AWS environment.
2. Create a connection to AWS.
3. Create a master image (AMI) enabled with NitroTPM and/or UEFI secure boot.
4. Create a prepared image from the master image. See Create a prepared image for Amazon WorkSpaces Core Managed Instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Create a machine catalog by selecting the prepared image with NitroTPM and UEFI secure boot enabled in Citrix Studio catalog creation menu or when creating a Provisioning Scheme using PowerShell commands.

VMs added to the created catalog have NitoTPM and UEFI secure boot enabled.

Create an AMI that supports NitroTPM and UEFI secure boot

1. You can create an AMI from a VM that has NitroTPM and/or UEFI secure boot enabled.
   a. Create the instance from using the AWS marketplace images. Example, search for `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`.
   b. Download single or multi session VDA.
   c. Create an AMI from that VM.
2. Use the register-image command:

   ```
   --boot-mode (string)

   --tpm-support (string)
   ```

   For more information, see register-image.

See the following AWS documents:

- Determine the supported boot modes of an EC2 instance type
- Requirements for using NitroTPM with Amazon EC2 instances/.

You can open a PowerShell window from the Delivery controller™ host to check if a specific:

- service offering supports NitroTPM or UEFI secure boot

  ```
  (Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
  Instance.serviceoffering”).AdditionalData.BootMode

  (Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
  Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
  ```

- template supports NitroTPM or UEFI secure boot

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

Update the service offering of existing catalog

You can change the service offering of an existing catalog using `Set-ProvScheme`. The change applies to the newly added VMs. However, you get errors in the following scenarios:

AMIS BOOT MODE	AMI SUPPORTS NITRO TPM?	SERVICE OFFERING SUPPORTS NITROTPM AND UEFI SECURE BOOT?
UEFI	No	No
Legacy BIOS	Yes	No
UEFI	Yes	No
UEFI Preferred	Yes	No

Copy tags on VMs

You can copy tags on NICs, and disks (Identity disk, write back cache disk, and OS disk) that are specified in the machine profile to newly created VMs in an MCS machine catalog. You can specify these tags in any of the machine profile sources (AWS VM instance or AWS launch template version). This feature is applicable to persistent and non-persistent machine catalogs and VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- On the AWS EC2 console, you cannot see the **Tag Network Interfaces** values under the **Launch Template Version Resource Tags**. However, you can run the PowerShell command `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` to see the tag specifications.
- If a machine profile source (VM or launch template version) has two network interfaces (eni-1 and eni-2), and eni-1 has tag t1 and eni-2 has tag t2, then the VM gets both the two network interfaces' tags.

Filter VM instances using PowerShell

An AWS VM instance that you use as a machine profile VM must be compatible for the machine catalog to create and function correctly. To list the AWS VM instances that can be used as machine profile input VMs, you can use the `Get-HypInventoryItem` command. The command can page and filter the inventory of VMs available on a hosting unit.

Pagination:

Get-HypInventoryItem supports two modes of pagination:

- Paging mode uses the `-MaxRecords` and `-Skip` parameters to return sets of items:
  - `-MaxRecords`: The default is **1**. This controls how many items to return.
  - `-Skip`: The default is **0**. This controls how many items to skip from the absolute beginning (or absolute end) of the list in the hypervisor.
- Scrolling mode uses `-MaxRecords`, `-ForwardDirection`, and `-ContinuationToken` parameters to allow scrolling of the records:
  - `-ForwardDirection`: The default is **True**. This is used along with `-MaxRecords` to return either the next set of matching records or the previous set of matching records.
  - `-ContinuationToken`: The returns the items immediately after (or before if `ForwardDirection` is **false**) but not including the item given in the `ContinuationToken`.

Examples of pagination:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To return a single record of the machine template with the lowest name. The `AdditionalData` field has the `TotalItemsCount` and the `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- To return 10 records of the machine template with the lowest name:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- To return an array of records ending with the highest name:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- To return an array of records starting at the machine template associated with the given `ContinuationToken`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

Filtering:

The following additional optional parameters are supported for filtering. You can combine these parameters with the pagination options.

- `-ContainsName "my_name"`: If the given string matches part of an AMI name, then the AMI is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: If an AMI has at least one of these tags, it is included in the `Get` result. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

NOTE:

Two tag values are supported. **Not Tagged** tag value matches items which do not have the given tag in their list of tags. **All values** tag value matches items which have the tag regardless of the value of the tag. Otherwise, the match happens only if the item has the tag and the value equals to what is given in the filter.

- `-Id "ami-0a2d913927e0352f3"`: If the AMI matches the given ID, it is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

Filtering on AdditionalData parameter:

The `AdditionalData` filter parameter lists templates or VMs based on their capability, service offering, or any property which is in AdditionalData. For example:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

You can also add a `-Warn` parameter to indicate the incompatible VMs. The VMs are included with an `AdditionalData` field named **Warning**. For example:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

Where to go next

- For managing an Amazon Workspaces Core catalog, see Manage a catalog of Amazon WorkSpaces Core Managed Instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More information

- AWS virtualization environments
- Connection to Amazon WorkSpaces Core Managed Instances
- Image management
- Create a prepared image for Amazon WorkSpaces Core Managed Instances
- For Amazon WorkSpaces Core GitHub PowerShell examples, see citrix-mcs-sdk-samples-Amazon WorkSpaces Core.

Create an Amulet Hotkey CoreStation machine catalog

Create machine catalogs describes the generic machine-catalog workflow. The following information covers Amulet Hotkey CoreStation specific details.

NOTE:

- Before creating an Amulet Hotkey CoreStation catalog, complete Connection to Amulet Hotkey CoreStation.
- Make sure to have one or more Amulet Hotkey CoreStation nodes available and install VDAs on those nodes.
- For information about creating the initial Amulet Hotkey CoreStation cartridge image, see the OS Deployment on CoreStation User Guide.

You can create an Amulet Hotkey CoreStation machine catalog using:

- Studio
- PowerShell commands

Using Studio

In the Machine Catalog Setup wizard:

1. On the **Operating System** page, select **Multi-session OS** or **Single-session OS**.
2. On the **Machine Management** page, select **Machines that are power managed and Another service or technology**.
3. On the **Virtual Machines** page, add machines and their Active Directory machine accounts. You can do either of the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Click **Add Machines** to add machines manually. The **Select VMs window** appears. Expand the Amulet Hotkey CoreStation enclosure connection you created earlier and select the nodes you want to add. Then add the associated machine account names.
- Click **Add CSV File** to bulk add machines. For information about using CSV files to add machines, see Use CSV files to bulk add machines to a catalog.

The **Scopes** and **Summary** pages do not contain Amulet Hotkey CoreStation-specific information.

Using PowerShell commands

Run `New-BrokerCatalog` and `New-BrokerMachine` PowerShell commands to create a broker catalog and import machines to the broker catalog.

For example:

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To power manage, see Power manage Amulet Hotkey CoreStation VMs.

More information

- Create and manage connections and resources
- Connection to Amulet Hotkey CoreStation
- Create machine catalogs

Create an AWS EC2 catalog

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to AWS EC2 virtualization environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Before creating an AWS catalog, you need to finish creating a connection to AWS. See Connection to AWS EC2.

Network setting during image preparation

During image preparation, a preparation virtual machine (VM) is created based on the original VM. This preparation VM is disconnected from the network. To disconnect the network from the preparation VM, a network security group is created to deny all inbound and outbound traffic. This network security group persists and is reused. The network security group's name is `Citrix.XenDesktop.IsolationGroup-GUID`, where GUID is randomly generated.

AWS tenancy

AWS provides the following tenancy options:

- Shared tenancy (the default type) and dedicated tenancy. Shared tenancy means that multiple Amazon EC2 instances from different customers might reside on the same piece of physical hardware.
- Dedicated tenancy means that your EC2 instances run only on hardware with other instances that you have deployed. Other customers do not use the same piece of hardware.

Requirements for provisioning to AWS hosts

- An imported BYOL (bring your own license) image (AMI). With dedicated hosts, use and manage your existing licenses.
- An allocation of dedicated hosts with sufficient utilization to satisfy provisioning requests.
- Enabling **auto-placement**.

Options to configure AWS tenancy

- **Use shared hardware**. This setting is suitable for most deployments. Multiple customers share pieces of hardware even though they do not interact with each other. Using shared hardware is the least expensive option for running your Amazon EC2 instances.
- **Use dedicated host**. An Amazon EC2 dedicated host is a physical server with EC2 instance capacity that is fully dedicated, letting you use existing per-socket or per-VM software licenses. Dedicated hosts have preset utilization based on instance type. For example, a single allocated dedicated host of C4 Large instance types is limited to running 16 instances. See the AWS site for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This setting is suitable for deployments with licensing restrictions or security requirements that need your use of a dedicated host. With a dedicated host, you own an entire physical host and are billed on an hourly basis. Owning that host lets you spin up as many EC2 instances as that host permits, without more charges.

- **Use dedicated instance**. This setting is more suitable for deployments with specific security or compliance requirements. With a dedicated instance, you still enjoy the benefits of having a host separate from other AWS customers but you do not pay for the entire host. You do not need to worry about the capacity of the host but you are charged at a higher rate for the instances.

NOTE:

You can delete any available preparation identity disk if there is no ongoing catalog creation or image update task.

To configure AWS tenancy using Studio, see Create a catalog using Studio and using PowerShell, see Configure AWS dedicated host tenancy using the PowerShell.

Tag AWS operational resources

An Amazon Machine Image (AMI) represents a type of virtual appliance used to create a virtual machine within the Amazon Cloud environment, commonly referred to as EC2. You use an AMI to deploy services that use the EC2 environment. When you create a catalog to provision machines using MCS for AWS, you select the **AMI** to act as the golden image for that catalog.

IMPORTANT:

Creating catalogs by using both a machine profile and a launch template is required for using operational resource tagging.

To create an AWS catalog, you must first create an AMI for the instance you want to be the golden image. MCS reads the tags from that instance and incorporates them into the launch template. The launch template tags are then applied to all Citrix® resources created in your AWS environment, including:

- Virtual Machines
- VM disks
- VM network interfaces

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- S3 buckets
- S3 objects
- Launch templates
- AMIs

You can tag operational resources using Studio and PowerShell while creating a catalog. For Studio, see Create a catalog using Studio (**Image** page). For PowerShell, see Tag operational resources using PowerShell.

Create a catalog

You can create a catalog using:

- Studio
- PowerShell

Create a catalog using Studio

1. Click **Machine Catalogs** on the left navigation pane.
2. Click **Create Machine Catalog**. The **Machine Catalog Setup** page appears.
3. On the **Machine Type** page, select a machine type for the catalog, for example, Multi-session OS.
4. On the **Machine Management** page, select the following settings:
    a. Select Machines that are power managed (for example, virtual machines or blade PCs).
    b. Select **Citrix provisioning technology**. Then, select **Citrix Machine Creation Services™**.
    c. In the **Resources** field, select the resources (Availability Zone or Local Zone) that you configured while creating the host connection and click **Next**.
5. On the **Desktop experience** page, select either random or static desktop that you want users to have when they log in.
6. On the **Image** page:
    a. Select a machine template that you want to use as the master image for all machines in the catalog.
    b. If you want VMs in the catalog to inherit configurations from a machine profile, select a machine profile. By default, the **Use a machine profile** checkbox is selected. To change the machine profile source to another VM or launch template version, click the edit button.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. If the machine template has two volumes, then the option **Provision a Data disk** is enabled by default. In this case, machine profiles are filtered with only those instances or launch templates with two volumes (that specifies the hardware properties, for example, block device mapping, volume type) for the two volumes, and launch templates with no volumes and block device mappings defined.

   If you clear the checkbox to provision a data disk, then machine profiles are filtered with only those launch templates with no volumes and block device mappings defined.

   For a machine profile-based MCS catalog, you can use the same master VM as the data disk source for the machine profile.

d. Select the **Apply machine tags to operational resources** checkbox to apply machine tags to operational resources. This option controls whether to apply machine tags to every item created in your AWS environment that facilitates provisioning of machines. Operational resources are created as byproducts of catalog creation. They include both temporary and persistent resources, such as preparation VM instances and AMI.

NOTE:

The **Security** page appears only if you are creating a machine catalog without assigning a machine profile.

7. On the **Virtual Machines** page:

   a. Enter the number of VMs for the catalog.

   b. The default machine specification is displayed, which is based on the machine profile. To change it, select the edit icon and select a machine specification.

   c. Configure the AWS tenancy. See Options to configure AWS tenancy.

   d. You can also configure a secondary VM when the primary machine size reaches full capacity. Click **Secondary size** (optional). In the **Secondary machine size** window, the VMs listed have both, Spot and Regular VM types. You may select up to 10 secondary machine sizes. Once the 10 VMs are selected, then the other VMs listed are disabled from further selection. Click **Next**. In the **Secondary machine size** blade, you can select multiple machine sizes and drag and drop to change the priority order. Click **Done**. The selected machine sizes show up in the Secondary size (optional). Click the edit icon to edit as needed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. The **Security** page appears only if you are creating a machine catalog without assigninga machine profile. Use the **Security** page to configure the security groups for the VMs. This is also applicable when editing and cloning an existing machine catalog.

   If you create a machine profile-based machine catalog, then the security group configurations are inherited from the machine profile and the **Security** page does not appear.
9. In the **NICs** page, select the NICs (or ENIs) for the VMs.
10. On the **Disk Settings** page, choose whether to enable write-back cache.
11. On the **Machine Identities** page, configure on-premises Active Directory or Microsoft Entra hybrid joined for the machines in the catalog by selecting the domain and creating new AD accounts for the VMs to be created in this machine catalog. The provisioned VMs are joined to the domain selected. Specify the account naming scheme for the new AD accounts to be created for the VMs. Click Next.
12. On the **Domain credentials** page, click **Enter credentials** to provide the credentials for the selected domain. Enter admin-level username and password when prompted. You can also use a service account if you have domain credentials already saved previously by following our product docs.
13. Click through the remaining pages until the **Summary** page. If you select to provision a data disk on the **Images** page, the value of **Use data disk** is set to **true** on the **Summary** page.Enter a name for the machine catalog and select **Finish** to create the machine catalog.

Limitations on creating a machine catalog in an AWS local zone

- Certain local zones only support certain hardware configurations (for example, Perth local zone does not support GP3 volumes, only GP2).
- Since only gp2 is universally supported across all local zones, and not all support gp3, ID disk creation defaults to using gp2 volume type.
- You must select a machine profile with hardware specifications that are supported in the desired local zone.
- Prepared image AMIs snapshots and ID disk snapshots defaults to being placed in the region, rather than the local zone (due to AWS limitations regarding visibility into EBS snapshot support in local zones).
- Only local zones supporting full EC2 and EBS services are supported zones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a catalog using PowerShell

Configure AWS dedicated host tenancy using the PowerShell

Alternatively, you can provision AWS dedicated hosts through PowerShell. Use the `New-ProvScheme` cmdlet with the parameter `TenancyType` set to `Host`.

Tag operational resources using PowerShell

To use PowerShell to tag resources:

1. Open a PowerShell window from the DDC host.
2. Run the command `asnp citrix` to load Citrix-specific PowerShell modules.

To tag a resource for a provisioned VM, use the custom property `AwsOperationalResourcesTagging`. Example:

```
New-ProvScheme -ProvisioningSchemeName test

-CustomProperties “AwsOperationalResourcesTagging,true”

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"

... <Other <standard provscheme parameters>
```

MCSIO enabled catalog

MCS Storage Optimization (MCSIO) improves the performance of the VM by caching disk operations in either memory or on a small, high-speed disk. You can create an MCSIO enabled non-persistent catalog using PowerShell commands. To create such a catalog, you must install the MCSIO driver while installing or upgrading the VDA during the preparation of the AMI instance. By default, that driver is not installed.

After an MCSIO AMI is prepared (when installing the VDA, select the option to include the MCSIO driver in the installation), you can create an MCSIO enabled non-persistent catalog.

NOTE:

The option to configure MCSIO with only disk cache (without memory cache) using Studio has been removed across all hypervisors and cloud service environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create an MCSIO enabled catalog

The four parameters added to the New-ProvScheme PowerShell command are:

- `UseWriteBackCache`: Turns on caching (write-back cache) for the given provisioning scheme
- `WriteBackCacheDiskSize`: Specifies the size in GB of the temporary disk used for caching
- `WriteBackCacheMemorySize`: Specifies how much memory in MB to use for caching. This is an optional parameter.

NOTE:

- The value of `WriteBackCacheDiskSize` must be more than zero because at least 1 GB of cache disk storage is required. The cache disk size must not be bigger than the OS disk size.
- The value of `WriteBackCacheMemorySize` must be non-zero and less than the machine catalog memory size.

The custom properties that affect MCSIO are:

- `WBCDiskStorageType`: Defines the volume type, which is used for the temporary disk in AWS. This parameter takes a string argument in the format `volume-type[:iops][:throughput]`. The following are the volume types:
  - gp2: Do not use iops and throughput parameters for this volume type
  - gp3: Use iops and throughput parameters for this volume type
  - io1: Use only iops parameter for this volume type
  - io2: Use only iops parameter for this volume type

  The default volume type is **gp2**.
- `PersistWBC`: Controls whether to keep or discard the cache disk whenever the AWS instance is powered off. If set to `true`, the cache disk is kept. If set to `false` (the default), the cache disk is only created and kept while the AMI instance is powered on.
- `PersistOSDisk`: Controls whether to keep or discard the OS disk whenever the AWS instance is powered off. If set to `true`, the OS disk is kept. If set to `false` (the default), the OS disk is only created and kept while the AMI instance is powered on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Perform the following steps in the PowerShell window to create an MCSIO enabled non-persistent catalog:

1. Open the PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create a broker catalog and an identity pool.
4. Create the provisioning scheme. For example:

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'




$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. Add VMs to the catalog.

Improve boot performance with MCSIO

You can improve the boot performance of VMs if you enable MCSIO and set `PersistWBC` and `PersistOSDisk` custom properties as `tru`e. With such a setting, VMs can boot faster because they do not need to initialize a new cache disk or to recreate a root disk from their template.

Create a machine profile-based machine catalog using PowerShell

You can use a machine profile to capture the hardware properties from an EC2 instance (VM) or launch template version and apply them to the provisioned machines. Properties that are captured can include, for example, EBS volume properties, instance type, EBS optimization, CPU options, tenancy type, hibernation capability, security groups, and other supported AWS configurations.

You can use an AWS EC2 Instance (VM) or AWS Launch Template version as the machine profile input.

NOTE:

EBS volume properties are derived only from a machine profile.

Important considerations

The important considerations while creating an MCS machine catalog:

- If you add machine hardware property parameters in the `New-ProvScheme` and `Set-ProvScheme` commands, then the values provided in the parameters overwrite the values in the machine profile.
- If you set `AwsCaptureInstanceProperties` as `true` and do not set `MachineProfile` property, then only IAM roles and tags are captured.
- You cannot set both `AwsCaptureInstanceProperties` and `MachineProfile` at the same time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The `AwsCaptureInstanceProperties` is deprecated.

- If a machine profile is not provided, you must explicitly provide the values of the following properties:
  - Security Group
  - ENI or Virtual Network
- You can enable `AwsOperationalResourcesTagging` only if you enable `AwsCaptureInstanceProperties` or specify a machine profile.

The important consideration after creating an MCS machine catalog is:

- You cannot change a catalog from a machine profile-based to a non-machine profile-based catalog.

Configure security groups in a machine profile input

You can create an MCS machine catalog where the provisioned VMs are assigned security groups per ENI (Network Interface). To do this, use a machine profile input (EC2 instance or launch template) that has different security groups mapped to distinct ENIs. For example, if machine profile input has ENI A with SG 1 and ENI B with SG 2, then provisioned VMs must also have ENI A with SG 1 and ENI B with SG 2.

Retrieve network interface details

Run the following commands to get the list of network interface data records including the interface SubnetId, assigned security groups, and assigned networks.

```
(Get-HypInventoryItem -LiteralPath 'XdHyp:\HostingUnits\cvad-test' –
ResourceType vm). AdditionalData
```

NOTE:

MCS does not currently allow more than one network per network interface.

Create a machine catalog using a machine profile

To create a machine catalog using a machine profile:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create an identity pool if not already created. For example,

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. Run New-ProvScheme command. For example:

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. Complete creating the catalog.

Update the machine profile

To update the machine profile on a catalog that was initially provisioned with a machine profile, do the following. You can also change the tenancy type and hibernation capability of the machine profile source while editing an MCS machine catalog.

1. Run `Set-ProvScheme` command. For example,

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a catalog with launch template version using PowerShell

You can create an MCS machine catalog with a launch template version as a machine profile input. You can also update the input of a machine profile catalog from a VM to a launch template version and from a launch template version to a VM.

On the AWS EC2 console, you can provide the instance configuration information of a launch template along with version number. When you specify the launch template version as a machine profile input while creating or updating a machine catalog, the properties from that version of the launch template are copied to the provisioned VDA VMs.

The following properties can be provided using machine profile input or explicitly as parameters in `New-ProvScheme` or `Set-ProvScheme`commands. If they are provided in `New-ProvScheme` or `Set-ProvScheme` commands, they take precedence over the machine profile values of these properties.

- Service Offering
- Networks
- Tenancy Type

NOTE:

If service offering is not provided in the machine profile launch template or as a parameter in the `New-ProvScheme` command, you get an appropriate error.

To create a catalog using launch template version as a machine profile input:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Get the list of launch template versions of a launch template. For example:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. Create an identity pool if not created. For example:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. Create a provisioning scheme with a launch template version as a machine profile input. For example:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. Register a provisioning scheme as a broker catalog. For example:

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-PersistUserChanges Discard
```

7. Complete creating the catalog.

Update the machine profile source

You can also update the input of a machine profile catalog from a VM to a launch template version and from a launch template version to a VM. For example:

- To update the input of a machine profile catalog from a VM to a launch template version:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx
(1).launchtemplateversion"
```

- To update the input of a machine profile catalog from a launch template version to a VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

Encrypt OS, ID, and WBC disks

You can create a persistent and non-persistent catalog of VMs with AWS KMS keys (Customer managed key and AWS managed key) that can be used to encrypt OS disk, Identity Disk (ID), and write-back cache disk (WBC).

- AWS managed keys are automatically rotated every year.
- Customer managed keys are optional for automatic rotation and can be managed manually.

You can see the following AWS documents for more information on KMS keys:

- AWS KMS concepts
- How automatic key rotation works

For encryption of OS, ID, and WBC disks, configure one of the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Use a master image that is encrypted (for example, an AMI created from an instance or snapshot that contains an EBS root volume encrypted with KMS key)
- Use a machine profile source (VM or launch template) that contains an encrypted EBS root volume.

Limitations

Consider the following limitations:

- MCS currently supports only one disk on master image AMI.
- You cannot directly encrypt existing unencrypted EBS volumes or snapshots, or modify the KMS key of an existing encrypted volume. To do that, you must:
  a. Create a new snapshot of that volume.
  b. Create a new volume from that snapshot
  c. Encrypt the new volume.

See the following AWS documents:

- Encrypt unencrypted resources
- Limitations of automatic or default encryption of EBS volumes: Automatically encrypt existing and new Amazon EBS volumes.

Create a catalog with disk encryption

You can create an MCS machine catalog with disk encryption using:

- Master image
- Machine profile

Considerations while using machine profile input are:

- The KMS key of the machine profile input takes precedence over the master image's KMS key.
- If no machine profile input is provided, then the KMS key of the master image AMI is used to encrypt the disks of catalog VMs.
- If the machine profile has Block Device Mappings present, then the block devices present in the master image template (AMI) and the machine profile must match. For example, if AMI has a device defined on `/dev/sda1`, then the Machine Profile must also have a device defined on `/dev/sda1`.
- If there is no key in the machine profile source and the master image is unencrypted, then disks of catalog VMs are not encrypted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When the master image is encrypted, a machine profile source VM or launch template must have an encrypted root volume to be considered a valid input.

Modify an existing catalog

You can modify an existing catalog using the `Set-ProvScheme` PowerShell command to have:

- A machine profile input with a volume containing a new KMS key.
- A master image template AMI encrypted with a new KMS key.

Important considerations:

- The volumes of new VMs added to the catalog are encrypted with the new KMS key.
- To update the encryption settings when there is an existing machine profile, run `Set-ProvScheme` with a new machine profile.
- You cannot modify an existing catalog from having encrypted volumes to unencrypted volumes. You can't do an image update from an encrypted master AMI to an unencrypted master AMI.

Enable NitroTPM and UEFI secure boot for VM instances

When creating a catalog, you can now select a master image (AMI) with NitroTPM and/or UEFI secure boot enabled. Accordingly, the provisioned VMs in the catalog are also enabled with NitroTPM and/or UEFI secure boot. This implementation ensures that the VMs are secured and trusted. For more information on NitroTPM and UEFI Secure Boot, see the Amazon documentation.

Limitations

- You can use both NitroTPM and Secure Boot currently in all AWS Regions (including the AWS GovCloud (US) Regions) except China.
- You cannot enable NitroTPM and UEFI secure boot on existing catalogs. If you want a catalog with NitroTPM and UEFI secure boot enabled, create a new catalog.

Key steps

1. Set up your AWS environment.
2. Create a connection to AWS.
3. Create a master image (AMI) enabled with NitroTPM and/or UEFI secure boot.
4. Create a machine catalog by selecting the master image with NitroTPM and UEFI secure boot enabled in Web Studio catalog creation menu or when creating a Provisioning Scheme using PowerShell commands.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VMs added to the created catalog have NitoTPM and UEFI secure boot enabled.

Create an AMI that supports NitroTPM and UEFI secure boot

1. You can create an AMI from a VM that has NitroTPM and/or UEFI secure boot enabled.
   a. Create the instance from using the AWS marketplace images. Example, search for `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`.
   b. Download single or multi session VDA.
   c. Create an AMI from that VM.
2. Use the register-image command:

   ```
   --boot-mode (string)

   --tpm-support (string)
   ```

   For more information, see register-image.

See the following AWS documents:

- Determine the supported boot modes of an EC2 instance type
- Requirements for using NitroTPM with Amazon EC2 instances/.

You can open a PowerShell window from the Delivery controller™ host to check if a specific:

- service offering supports NitroTPM or UEFI secure boot

  ```
  (Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
  Instance.serviceoffering”).AdditionalData.BootMode

  (Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
  Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
  ```

- template supports NitroTPM or UEFI secure boot

  ```
  (Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
  -ResourceType “template -Id “ID”).AdditionalData.BootMode
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

Update the service offering of existing catalog

You can change the service offering of an existing catalog using `Set-ProvScheme`. The change applies to the newly added VMs. However, you get errors in the following scenarios:

AMIS BOOT MODE	AMI SUPPORTS NITRO TPM?	SERVICE OFFERING SUPPORTS NITROTPM AND UEFI SECURE BOOT?
UEFI	No	No
Legacy BIOS	Yes	No
UEFI	Yes	No
UEFI Preferred	Yes	No

Provision a data disk on MCS created VM

A data disk allows storage of persistent data like event logs, security traces, and application data.

You can create and assign a persistent data disk to an MCS created persistent or non-persistent VM of an MCS machine catalog in AWS.

You can provision persistent data disks with the OS and ID disks. And, the source of the data disk must be the master image (AMI's secondary volume).

You can create both machine profile and non-machine profile-based MCS catalog. For machine profile-based MCS catalog, you can use the same master image VM as the data disk source for the machine profile.

Data disk properties

The provisioned VM's data disk derives:

- Size and device name from the AMI
- Volume type from the AMI if the machine profile is not provided

For machine profile based catalog,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If the data disk is in the machine profile template, then provisioned VM derives data disk properties such as tag, storage policy, and storage tier from machine profile.
- The machine profile template must also have a data disk at the same device index as that of the data disk from the AMI

For non-machine profile based catalog, hardware information is derived from the master image AMI.

The data disk is also encrypted with a KMS key and inherits the KMS key of the data disk from AMI or machine profile if the KMS key is provided. The KMS of the machine profile though, takes precedence. You cannot change the KMS of the data disk.

Limitations

The following operations are currently not supported:

- Provisioning of non-persistent data disks.
- Using a machine profile:
  - with no data disk when the AMI has one, or
  - at a different data disk index than that of the AMI
- Per-disk tagging at instance creation time.
- Data disk device name restrictions:
  - For Windows AMIs, place the data disk on xvd and not on xvd
  - For Linux AMIs, place the data disk on /dev/sd and not on /dev/sd
- Modifying existing catalogs and VMs to use data disks.
- Resetting of data disk.
- Updating an image, of an existing catalog, that has a data disk with an image that doesn't have a data disk. Only new VMs are updated with image contents and volume properties, while existing VMs are not updated.
- Provisioning WBC disk with data disk.

Create a catalog with data disk

You can create a catalog with data disk using Studio and PowerShell.

For Studio, see Create a catalog using Studio. Additionally, see the following important points:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Create a master image (AMI) from a master VM with two volumes, one of the OS disk (root volume) and one for the data disk (secondary volume).
- For a machine profile-based MCS catalog, you can use the same master VM as the data disk source for the machine profile.
- During catalog creation in the Studio UI, select the AMI you created with two voumes as the master image
- The **Provision data disk** option is enabled by default.
- Select a machine profile with 2 volumes (instance or launch template) or 0 volumes (launch templates only) that specifies the hardware properites (for example, block device mapping, volume type) for the two volumes.
- You cannot provision a data disk when the master image (AMI) has:
  - One volume: In this case, machine profiles are filtered with only those instances or launch templates with 1 volume, and launch templates with no volumes and block device mappings defined.
  - More than 2 volumes: In this case, machine profiles are filtered with only those launch templates with no volumes and block device mappings defined
- Finish creating the catalog and data data disk will be provisioned for the VMs in the catalog

Use PowerShell SDK

1. Create a master image (AMI) from a master VM with a data disk in AWS.

   For a machine profile-based MCS catalog, you can use the same master VM as the data disk source for the machine profile.

2. Create an MCS machine catalog with data disk provisioned VMs using `New-ProvScheme` PowerShell command with `DataDiskPersistence` parameter value - `"Persistent"`. For example:

   ```
   New-ProvScheme  -CleanOnBoot -HostingUnitName "<HostingUnitName >"
   -IdentityPoolName "<IdentityPoolName >" -InitialBatchSizeHint 1
   -MasterImageVM "<Path to master image item with an additional disk >"
   -NetworkMapping <NetworkMapping > -ProvisioningSchemeName
   "<ProvisioningSchemeName >" -DataDisk "" -DataDiskPersistence
   "Persistent"  -Scope @() -VMCpuCount 4  -VMMemoryMB 6144  -TenancyType
   Shared  -FunctionalLevel "L7_20"
   ```

3. Add VMs to the catalog using the `New-ProvVM` PowerShell command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Image update with data disk

You can update the image using `Publish-ProvMasterVMImage`, however, you cannot update an image of an existing catalog, containing a data disk with an image that doesn't have a data disk. After you update the image:

- For a persistent catalog:
  - new VMs in the catalog have updated OS disk and data disk. Existing VMs are not updated
- For a non-persistent catalog:
  - new VMs in the catalog have updated OS disk and data disk. Existing VMs' OS disk is updated on the next restart, while the data disk is not updated.

Delete data disk

If you delete the catalog, the data disk is deleted unless you use `forgetVM` or `purgeDBOnly` option. If you delete the VM, the data disk is deleted unless you use the `forgetVM` or `purgeDBOnly` option.

For on-demand provisioning catalogs, never delete the data disk.

Copy tags on VMs

You can copy tags on NICs, and disks (Identity disk, write back cache disk, and OS disk) that are specified in the machine profile to newly created VMs in an MCS machine catalog. You can specify these tags in any of the machine profile sources (AWS VM instance or AWS launch template version). This feature is applicable to persistent and non-persistent machine catalogs and VMs.

NOTE:

- On the AWS EC2 console, you cannot see the **Tag Network Interfaces** values under the **Launch Template Version Resource Tags**. However, you can run the PowerShell command `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` to see the tag specifications.
- If a machine profile source (VM or launch template version) has two network interfaces (eni-1 and eni-2), and eni-1 has tag t1 and eni-2 has tag t2, then the VM gets both the two network interfaces' tags.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filter VM instances using PowerShell

An AWS VM instance that you use as a machine profile VM must be compatible for the machine catalog to create and function correctly. To list the AWS VM instances that can be used as machine profile input VMs, you can use the `Get-HypInventoryItem` command. The command can page and filter the inventory of VMs available on a hosting unit.

Pagination:

Get-HypInventoryItem supports two modes of pagination:

- Paging mode uses the `-MaxRecords` and `-Skip` parameters to return sets of items:
  - `-MaxRecords`: The default is **1**. This controls how many items to return.
  - `-Skip`: The default is **0**. This controls how many items to skip from the absolute beginning (or absolute end) of the list in the hypervisor.
- Scrolling mode uses `-MaxRecords`, `-ForwardDirection`, and `-ContinuationToken` parameters to allow scrolling of the records:
  - `-ForwardDirection`: The default is **True**. This is used along with `-MaxRecords` to return either the next set of matching records or the previous set of matching records.
  - `-ContinuationToken`: The returns the items immediately after (or before if `ForwardDirection` is **false**) but not including the item given in the `ContinuationToken`.

Examples of pagination:

- To return a single record of the machine template with the lowest name. The `AdditionalData` field has the `TotalItemsCount` and the `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- To return 10 records of the machine template with the lowest name:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- To return an array of records ending with the highest name:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- To return an array of records starting at the machine template associated with the given `ContinuationToken`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

Filtering:

The following additional optional parameters are supported for filtering. You can combine these parameters with the pagination options.

- `-ContainsName "my_name"`: If the given string matches part of an AMI name, then the AMI is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: If an AMI has at least one of these tags, it is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

NOTE:

Two tag values are supported. **Not Tagged** tag value matches items which do not have the given tag in their list of tags. **All values** tag value matches items which have the tag regardless of the value of the tag. Otherwise, the match happens only if the item has the tag and the value equals to what is given in the filter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `-Id "ami-0a2d913927e0352f3"`: If the AMI matches the given ID, it is included in the `Get` result. For example:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

Filtering on AdditionalData parameter:

The `AdditionalData` filter parameter lists templates or VMs based on their capability, service offering, or any property which is in AdditionalData. For example:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

You can also add a `-Warn` parameter to indicate the incompatible VMs. The VMs are included with an `AdditionalData` field named **Warning**. For example:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

Backup SKU list for VMs

Public clouds can sometimes run out of capacity for a specific EC2 instance type (“primary SKU”). If the primary VM configuration is not available, then the VM cannot start resulting in loss of time and business disruption. To address such scenarios, provide a list of backup EC2 instance types (“backup SKUs”) that MCS can fall back to in the case of capacity-related issues.

Use a custom property `BackupVmConfiguration` while creating or updating an MCS machine catalog to provide a list of backup EC2 instance types (“Backup SKU List”).

If the primary EC2 instance fails, MCS attempts to fall back on the backup EC2 instance types in the order you specify. If MCS is unable to fall back on any of the provided backup EC2 instance types, an error message is displayed. You can then try powering on the primary EC2 instance again. If this fails, MCS retries the backup EC2 instance types.

The backup SKU list can have on-demand instance.

This feature is applicable to both persistent and non-persistent MCS machine catalogs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Important considerations

- You can provide multiple backup EC2 instance types in the backup SKU list.
- The backup SKU list must be unique.
- A backup EC2 instance cannot be the same as the primary EC2 instance.
- The backup EC2 instances must be valid AWS instance types.
- Do not specify duplicate service offerings. Example: `BackupVmConfiguration,t2.small|t3.small|t2.small` is not valid.
- The service offering specified in the list must be compatible with the machine catalog configuration. For example, if the catalog uses UEFI and the service offering specified in the backup list doesn't support it, then the catalog creation or update fails during preflight.
- You can modify the backup SKU list of an existing catalog using the `Set-ProvScheme` PowerShell command. You can modify existing VMs using the `Set-ProvVM` and `Set-ProvVMUpdateTimeWindow` PowerShell commands.

Configure backup EC2 instances

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create a Broker catalog.
4. Create an identity pool.
5. Add a backup EC2 instance list using the custom property `BackupVmConfiguration` and create a provisioning scheme. For example:

```
$serviceOffering = "XDHyp:\HostingUnits\$hostingUnitName\T3 Medium
Instance.serviceoffering"

$customProperties =
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small|t3.large;"

$createdProvScheme = New-ProvScheme -ProvisioningSchemeName
$provisioningSchemeName -HostingUnitName $hostingUnitName
-IdentityPoolName $provisioningSchemeName -NetworkMapping
$networkMapping -SecurityGroup $securityGroupPath -ServiceOffering
$serviceOffering -MasterImageVM $masterImageVm -CustomProperties
$customProperties
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Update the BrokerCatalog with the unique Id of the provisioning scheme.
7. Create and add VMs to the catalog.

You can also add backup EC2 instances using Studio:

On the **Virtual Machines** page, click **Secondary size** (optional). In the **Secondary machine size** window, the VMs listed have both, Spot and Regular VM types. You may select up to 10 secondary machine sizes. Once the 10 VMs are selected, then the other VMs listed are disabled from further selection. Click **Next**. In the **Secondary machine size** blade, you can select multiple machine sizes and drag and drop to change the priority order. Click **Done**. The selected machine sizes show up in the Secondary size (optional). Click the edit icon to edit as needed. See Create a catalog using Studio.

Create a catalog using AWS Spot instance

Compared to On-demand instances, Spot instances offer cost savings of up to 90%. Spot instances may be interrupted by Amazon EC2 if capacity becomes unavailable, making them suitable for non-critical applications and desktops only.

For information on Spot instances, see the AWS doc Spot Instances.

Additionally, you can use Spot instances as both primary EC2 instance type and backup EC2 instance. You can provide a list of backup EC2 instance types (“Backup SKUs” that can be On-demand and Spot instances) using PowerShell that MCS can fall back to in capacity-related issues.

Important considerations**

- You must create a catalog of Spot instances only with machine profile workflow.
- Only a persistent Spot instance request type is supported. A one-time Spot Instance request is not supported.
- Only the **Stop** and **Hibernate** interruption behaviors are supported.
- You can change the configuration of an existing catalog from On-demand to Spot instances and vice versa. However, changing an EC2 instance from On-demand to Spot is complex. See the AWS documentation Switch an EC2 instance from on-demand to spot pricing.
- When you delete a provisioned Spot instance, cancel the existing spot instance request. Or else, AWS creates a new Spot instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Steps to create a catalog using AWS Spot instances

1. Create a machine profile source with Spot instance. For steps to create a Spot instance, see Create a Spot Instance request.
2. Create a machine catalog using a machine profile with `New-ProvScheme` PowerShell command. You can update a catalog using the `Set-ProvScheme` command.

Use Spot instances as backup SKU

You can use Spot instances as both primary EC2 instance type and backup EC2 instance. You can provide a list of backup EC2 instance types (“Backup SKUs” that can be On-demand and Spot instances) using PowerShell that MCS can fall back to in capacity-related issues.

NOTE:

You can specify duplicate Spot instances in the backup SKUs list. Example: `BackupVmConfiguration,t2.small:Spot|t2.small|t3.small` is valid.

Required permissions

You need the following permissions if you use Spot instance as a primary or backup EC2 instance:

- `ec2:DescribeSpotInstanceRequests`
- `ec2:CancelSpotInstanceRequests`

Configure backup Spot instances

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create a Broker catalog.
4. Create an identity pool.
5. Add a backup EC2 instance list using the custom property `BackupVmConfiguration` and create a provisioning scheme. For example:

```
$serviceOffering \= "XDHyp:\\HostingUnits\\$hostingUnitName\\T3 Medium
Instance.serviceoffering"

$customProperties \=
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small:Spot|t3.large:Spot"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$createdProvScheme \= New-ProvScheme \-ProvisioningSchemeName
$provisioningSchemeName \-HostingUnitName $hostingUnitName \-
IdentityPoolName $provisioningSchemeName \-NetworkMapping
$networkMapping \-SecurityGroup $securityGroupPath \-ServiceOffering
$serviceOffering \-MasterImageVM $masterImageVm \-CustomProperties
$customProperties
```

6. Update the BrokerCatalog with the unique Id of the provisioning scheme.
7. Create and add VMs to the catalog.

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage an AWS EC2 catalog.

More information

- Create and manage connections and resources
- Connection to AWS EC2
- Create machine catalogs

Create a Google Cloud Platform catalog

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Google cloud environments.

NOTE:

Before creating a Google cloud platform (GCP) catalog, you need to finish creating a connection to GCP. See Connection to Google cloud environments.

Prepare a master VM instance and a persistent disk

TIP:

Persistent disk is the Google Cloud term for virtual disk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To prepare your master VM instance, create and configure a VM instance with properties that match the configuration you want for the cloned VDA instances in your planned machine catalog. The configuration does not apply only to the instance size and type. It also includes instance attributes such as metadata, tags, GPU assignments, network tags, and service account properties.

As part of the mastering process, MCS uses your master VM instance to create the Google Cloud *instance template*. The instance template is then used to create the cloned VDA instances that comprise the machine catalog. Cloned instances inherit the properties (except the VPC, subnet, and persistent disk properties) of the master VM instance from which the instance template was created.

After configuring the properties of the master VM instance to your specifics, start the instance and then prepare the persistent disk for the instance.

We recommend that you manually create a snapshot of the disk or an image of the disk. Doing so lets you use a meaningful naming convention to track versions, gives you more options to manage earlier versions of your master image, and saves time for machine catalog creation. If you do not create your own snapshot, MCS creates a temporary snapshot for you (which is deleted at the end of the provisioning process). Manually creating a multi-regional snapshot of the OS disk or image also allows you to use the same master image for machine catalogs in different GCP regions.

Enable zone selection

Citrix DaaS™ supports zone selection. With zone selection, you specify the zones where you want to create VMs. With zone selection, administrators can place sole tenant nodes across zones of their choice. To configure sole tenancy, you must complete the following on Google Cloud:

- Reserve a Google Cloud sole-tenant node
- Create the VDA master image

Reserve a Google Cloud sole-tenant node

To reserve a sole-tenant node, refer to the Google Cloud documentation.

IMPORTANT:

A node template is used to indicate performance characteristics of the system that is reserved in the node group. Those characteristics include the number of vGPUs, the amount of memory allocated to the node, and the machine type used for machines created on the node. For more information see the Google Cloud documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create the VDA master image

To deploy machines on the sole-tenant node successfully, you need to take extra steps when creating a master VM image. Machine instances on Google Cloud have a property called *node affinity labels*. Instances used as master images for catalogs deployed to the sole-tenant node require a *node affinity label* that matches the name of the **target node group**. To achieve this, keep the following in mind:

- For a new instance, set the label in the Google Cloud console when creating an instance. For details, see Provision a sole-tenant VM.
- For an existing instance, set the label by using the **gcloud** command line. For details, see Configure node affinity labels.

NOTE:

If you intend to use sole tenancy with a shared VPC, see Shared Virtual Private Cloud.

Create a machine catalog

NOTE:

Create your resources before you create a machine catalog. Use the naming conventions established by Google Cloud when configuring machine catalogs. See Bucket and object naming guidelines for more information.

You can create a machine catalog in two ways:

- Studio
- PowerShell. See Manage Citrix DaaS using Remote PowerShell SDKs. For information on how to implement specific features using PowerShell, see Use PowerShell

Create a machine catalog using Studio

Follow the guidance in Create machine catalogs. The following description is unique to Google Cloud catalogs.

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select **Create Machine Catalog** in the action bar.
3. On the **Machine Type** page, select **Multi-session OS** and then select **Next**. Citrix DaaS also supports single-session OS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. On the **Machine Management** page, select the **Machines that are power managed** and the **Citrix Machine Creation Services™** options and then select **Next**. If there are multiple resources, select one from the menu.
5. On the **Image** page, complete these steps as needed, and then click **Next**.

    a. Select the master image. You can select the following image types:

    - Virtual Machine (whose regions are the same as the selected hosting units).
    - Snapshots (support multi-region snapshots).
    - OS image (support multi-region public and non-public images). If you want to use the sole tenancy functionality, be sure to select an image whose node group property is correctly configured. See Enable zone selection.

    b. On the **Select a machine profile** page, select resources from **Virtual machine** tab or from **Instance templates** tab.

    NOTE:

    - Currently, VMs in this catalog inherit the storage, machine type, and disk encryption, settings from the selected machine profile.
    - If you select an instance template as the machine profile, then all the zones are selected by default. You can select the zones as required.

    c. Select the minimum functional level for the catalog.

6. On the **Storage** page, select the type of storage used to contain the operating system for this machine catalog. Each of the following storage options has unique price and performance characteristics. An identity disk is always created using the zonal standard persistent disk.

    - Standard persistent disk
    - Balanced persistent disk
    - SSD persistent disk

    For details about Google Cloud storage options, see Storage options.

7. On the **Virtual Machines** page, specify how many VMs you want to create, view the detailed specification of the VMs, select the Google Cloud machine type, and then select **Next**. If you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

use sole tenant node groups for machine catalogs, be sure to select **only** the zones where reserved sole tenant nodes are available. See Enable zone selection.

NOTE

.

Google Cloud machine type is automatically selected based on the machine profile chosen. You can select a different machine type if necessary.

8. On the **Disk Settings** page, you can configure the following settings:

   - Choose whether to enable write-back cache. After enabling write-back cache, you can do the following:

     - Configure the size of the disk and RAM used for caching temporary data. For more information, see Configure cache for temporary data.
     - Select the storage type for the write-back cache disk. The following storage options are available to use for the write-back cache disk:

       - Standard persistent disk
       - Balanced persistent disk
       - SSD persistent disk

       For details about Google Cloud storage options, see Storage options.
     - Select the type for the write-back cache disk.

       - **Use non-persistent write-back cache disk**. If selected, the write-back cache disk does not persist for the provisioned VMs. The disk is deleted during power cycles and any data redirected to the disk will be lost.
       - **Use persistent write-back cache disk**. If selected, the write-back cache disk persists for the provisioned VMs. Enabling this option increases your storage costs.

   - When MCS storage optimization (MCS I/O) is enabled, you can do either of the following:

     - Choose whether to retain system disks for VDAs during power cycles. For more information, see Enabling MCS storage optimization updates.
     - Update the memory and disk cache sizes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Choose whether to use your own key to protect disk contents. To use the feature, you must first create your own Customer Managed Encryption Keys (CMEKs). For more information, see Use Customer Managed Encryption Keys (CMEK).

  NOTE:

  It is available only in the Studio interface.

  After creating the keys, you can select one of those keys from the list. You cannot change the key after you create the catalog. Google Cloud does not support rotating keys on existing persistent disks or images. Therefore, after you provision a catalog, the catalog is tied to a specific version of the key. If that key is disabled or destroyed, the instances and disks encrypted with it become unusable until the key is reenabled or restored.

  The Customer-Managed Encryption Key (CMEK) settings follow a priority sequence as below:

  - Customized CMEK of a catalog takes the highest priority.
  - If the selected machine profile is encrypted, the CMEK settings automatically use the machine profile's CMEK as the next priority.
  - If the selected machine profile is not encrypted, the CMEK settings automatically use the master image's CMEK.

9. On the **Machine Identities** page, select an Active Directory account and then select **Next**.
   - If you select **Create new Active Directory accounts**, select a domain and then enter the sequence of characters representing the naming scheme for the provisioned VM computer accounts created in the Active Directory. The account naming scheme can contain 1–64 characters, and cannot contain blank spaces, or non-ASCII or special characters.
   - If you select **Use existing Active Directory accounts**, select **Browse** to navigate to the existing Active Directory computer accounts for the selected machines.
10. On the **Domain Credentials** page, select **Enter credentials**, type the user name and password, select **Save**, and then select **Next**.
    - The credential you type must have permissions to perform Active Directory account operations.
11. On the **Scopes** page, select scopes for the machine catalog and then select **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can select optional scopes or select **custom scope** to customize scopes as needed.

12. On the **Summary** page, confirm the information, specify a name for the catalog, and then select **Finish**.

> **NOTE:**
>
> The catalog name can contain 1–39 characters, and cannot contain only blank spaces or the characters `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`.

Machine catalog creation might take a long time to complete. When it completes, the catalog is listed. You can verify that the machines are created on the target node groups in the Google Cloud console.

Import manually created Google Cloud machines

Using this feature, you can:

- Import manually created Google Cloud multi-session OS machines into a Citrix DaaS catalog.
- Remove manually created Google Cloud multi-session OS machines from a Citrix DaaS catalog.
- Use existing Citrix DaaS power management capabilities to power manage Google Cloud Windows multi-session OS machines. For example, set a restart schedule for those machines.

This functionality does not require changes to an existing Citrix DaaS provisioning workflow, nor the removal of any existing feature.

It is recommended that you use MCS to provision machines in Studio instead of importing manually created Google Cloud machines.

Shared Virtual Private Cloud

Shared Virtual Private Clouds (VPCs) comprise a host project, from which the shared subnets are made available, and one or more service projects that use the resource. Shared VPCs are desirable options for larger installations because they provide centralized control, usage, and administration of shared corporate Google cloud resources. For more information, see the Google Documentation site.

With this feature, Machine Creation Services (MCS) supports provisioning and managing machine catalogs deployed to Shared VPCs. This support, which is functionally equivalent to the support currently provided in local VPCs, differs in two areas:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You must grant extra permissions to the Service Account used to create the host connection. This process allows MCS to access and use Shared VPC Resources. See New permissions required.
- You must create two firewall rules, one each for ingress and egress. These firewall rules are used during the image mastering process. See Firewall Rules.

For information on configuring shared VPC, see Configure the shared VPC.

New permissions required

A Google Cloud service account with specific permissions is required when creating the host connection. These additional permissions must be granted to any service accounts used to create Shared VPC based host connections.

TIP:

These additional permissions are not new to Citrix DaaS. They are used to facilitate the implementation of local VPCs. With Shared VPCs, these additional permissions allow access to other shared VPC resources.

A maximum of four extra permissions must be granted to the service account associated with the host connection to support Shared VPC:

- **compute.firewalls.list** - This permission is mandatory. It allows MCS to retrieve the list of firewall rules present on the Shared VPC.
- **compute.networks.list** - This permission is mandatory. It allows MCS to identify the Shared VPC networks available to the service account.
- **compute.subnetworks.list** – This permission is optional depending on how you use VPCs. It allows MCS to identify the subnets within the visible Shared VPCs. This permission is already required when using local VPCs but must also be assigned in the Shared VPC host project.
- **compute.subnetworks.use** - This permission is optional depending on how you use VPCs. It is necessary to use subnet resources in the provisioned machine catalogs. This permission is already required for using local VPCs but must also be assigned in the Shared VPC host project.

When using these permissions, consider that there are different approaches based on the type of permission used to create the machine catalog:

- Project-level permission:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - Allows access to all Shared VPCs within the host project.
  - Requires the permissions `compute.subnetworks.list` and `compute.subnetworks.use` must be assigned to the service account.

- Subnet-level permission:
  - Allows access to specific subnets within the Shared VPC.
  - Permissions `compute.subnetworks.list` and `compute.subnetworks.use` are intrinsic to the subnet level assignment and therefore do not need to be assigned directly to the service account.

Select the approach that matches your organizational needs and security standards.

TIP:

For more information about the differences between project-level and subnet-level permissions, see Service Project Admins.

Firewall Rules

During the preparation of a machine catalog, a machine image is prepared to serve as the master image system disk for the catalog. When this process occurs, the disk is temporarily attached to a virtual machine. This VM must run in an isolated environment that prevents all inbound and outbound network traffic. This is accomplished through a pair of deny-all firewall rules; one for ingress and one for egress traffic. When using Google Cloud local VPCs, MCS creates this firewall in the local network and applies it to the machine for mastering. After mastering completes, the firewall rule is removed from the image.

We recommend keeping the number of new permissions required to use Shared VPCs to a minimum. Shared VPCs are higher-level corporate resources and typically have more rigid security protocols in place. For this reason, create a pair of firewall rules in the host project on the shared VPC resources, one for ingress and one for egress. Assign the highest priority to them. Apply a new target tag to each of these rules, using the following value:

`citrix-provisioning-quarantine-firewall`

When MCS creates or updates a machine catalog, it searches for firewall rules containing this target tag. It then examines the rules for correctness and applies them to the machine used to prepare the master image for the catalog. If the firewall rules are not found, or the rules are found but the rules or their priorities are incorrect, a message similar to the following appears:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag ‘citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."
```

Configure the shared VPC

Before adding the Shared VPC as a host connection in Citrix DaaS's Studio, complete the following steps to add service accounts from the project you intend to provision into:

1. Create an IAM role.
2. Add a service account to the host project IAM role.
3. Add the cloud build service account to the shared VPC.
4. Create firewall rules.

CREATE AN IAM ROLE

Determine the access level of the role:

- *Project level access*, or
- A more restricted model using *subnet level access*.

Project level access for IAM role. For the project level IAM role, include the following permissions:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

To create a project level IAM role:

1. In the Google Cloud console, navigate to **IAM & Admin > Roles**.
2. On the **Roles** page, select **CREATE ROLE**.
3. On the **Create Role** page, specify the role name. Select **ADD PERMISSIONS**.
    a. On the **Add permissions** page, add permissions to the role, individually. To add a permission, type the name of the permission in the **Filter table** field. Select the permission and then select **ADD**.
    b. Select **CREATE**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Subnet-level IAM role. This role omits the addition of the permissions `compute.subnetworks.list` and `compute.subnetworks.use` after selecting **CREATE ROLE**. For this IAM access level, the permissions `compute.firewalls.list` and `compute.networks.list` must be applied to the new role.

To create a subnet level IAM role:

1. In the Google Cloud console, navigate to **VPC network** > **Shared VPC**. The **Shared VPC** page appears, displaying the subnets of the Shared VPC networks that the host project contains.
2. On the **Shared VPC** page, select the subnet that you want to access.
3. In the top-right corner, select **ADD MEMBER** to add a service account.
4. On the **Add members** page, complete these steps:
    a. In the **New members** field, type the name of your service account and then select your service account in the menu.
    b. Select the **Select a role** field and then **Compute Network User**.
    c. Select **SAVE**.
5. In the Google Cloud console, navigate to **IAM & Admin** > **Roles**.
6. On the **Roles** page, select **CREATE ROLE**.
7. On the **Create Role** page, specify the role name. Select **ADD PERMISSIONS**.
    a. On the **Add permissions** page, add permissions to the role, individually. To add a permission, type the name of the permission in the **Filter table** field. Select the permission, and then select **ADD**.
    b. Select **CREATE**.

ADD A SERVICE ACCOUNT TO THE HOST PROJECT IAM ROLE

After creating an IAM role, do the following steps to add a service account for the host project:

1. In the Google Cloud console, navigate to the host project and then to **IAM & Admin > IAM**.
2. On the **IAM** page, select **ADD** to add a service account.
3. On the **Add members** page:
    a. In the **New members** field, type the name of your service account and then select your service account in the menu.
    b. Select a role field, type the IAM role you created, and then select the role in the menu.
    c. Select **SAVE**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The service account is now configured for the host project.

ADD THE CLOUD BUILD SERVICE ACCOUNT TO THE SHARED VPC

Every Google Cloud subscription has a service account that is named after the project ID number, followed by `cloudbuild.gserviceaccount`. For example: `705794712345@cloudbuild.gserviceaccount`.

You can determine the project ID number for your project by navigating to **Cloud overview > Dashboard** in the Google Cloud console. The project ID and project number are displayed on the project Dashboard Project info card:

Perform the following steps to add the Cloud Build service account to the Shared VPC:

1. In the Google Cloud console, navigate to the host project and then to **IAM & Admin** > **IAM**.
2. On the **Permissions** page, select **ADD** to add an account.
3. On the **Add members** page, complete these steps:
    a. In the **New members** field, type the name of the Cloud Build service account and then select your service account in the menu.
    b. Select the **Select a role** field, type `Computer Network User`, and then select the role in the menu.
    c. Select **SAVE**.

CREATE FIREWALL RULES

As part of the mastering process, MCS copies the selected machine image and uses it to prepare the master image system disk for the catalog. During mastering, MCS attaches the disk to a temporary virtual machine, which then runs preparation scripts. This VM must run in an isolated environment that prohibits all inbound and outbound network traffic.

To create an isolated environment, MCS requires two *deny all* firewall rules (an ingress rule and an egress rule). Therefore, create two firewall rules (Ingress and Egress) in the *Host Project* as follows:

1. In the Google Cloud console, navigate to the host project and then to **VPC network > Firewall**.
2. On the **Firewall** page, select **CREATE FIREWALL RULE**.
3. On the **Create a firewall rule** page, complete the following:
    - **Name**. Type a name for the rule.
    - **Network**. Select the Shared VPC network to which the ingress firewall rule applies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Priority**. The smaller the value is, the higher the priority of the rule is. We recommend a small value (for example, 10).
- **Direction of traffic**. Select **Ingress**.
- **Action on match**. Select **Deny**.
- **Targets**. Use the default, **Specified target tags**.
- **Target tags**. Type `citrix-provisioning-quarantine-firewall`.
- **Source filter**. Use the default, **IP ranges**.
- **Source IP ranges**. Type a range that matches all traffic. Type `0.0.0.0/0`.
- **Protocols and ports**. Select **Deny all**.

4. Select **CREATE** to create the rule.
5. Repeat the steps to create another rule. For **Direction of traffic**, select **Egress**.

Use Customer Managed Encryption Keys (CMEK)

NOTE:

Support for CMEK in GCP is currently under Preview.

You can use Customer Managed Encryption Keys (CMEK) for MCS catalogs. When using this functionality, you assign the Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` role to the Compute Engine Service Agent. Citrix DaaS account must have the correct permissions in the project where the key is stored. See Assign permissions to Citrix DaaS account. Refer to Helping to protect resources by using Cloud KMS keys for more information.

Your Compute Engine Service Agent is in the following form: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`. This form is different than the default Compute Engine Service Account.

NOTE:

This Compute Engine Service Account might not appear in the Google Console **IAM Permissions** display. In such cases, use the `gcloud` command as described in Helping to protect resources by using Cloud KMS keys.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assign permissions to Citrix DaaS account

Google Cloud KMS permissions can be configured in various ways. You can either provide *project level* KMS permissions or *resource level* KMS permissions. See Permissions and roles for more information.

PROJECT LEVEL KMS PERMISSIONS

One option is to provide Citrix DaaS account with project-level permissions to browse Cloud KMS resources. To do this, create a custom role, and add the following permissions:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Assign this custom role to your Citrix DaaS account. This allows you to browse regional keys in the relevant project in the inventory.

RESOURCE LEVEL KMS PERMISSIONS

For the other option, resource level permissions, in the Google Cloud console, browse to the `cryptoKey` you use for MCS provisioning. Add Citrix DaaS account to a key ring or a key that you use for catalog provisioning.

TIP:

With this option, you cannot browse regional keys for your project in the inventory because Citrix DaaS account does not have project-level list permissions on the Cloud KMS resources. However, you can still provision a catalog using CMEK by specifying the correct `cryptoKeyId` in the `ProvScheme` custom properties. See Create a catalog with CMEK using custom properties.

Rotating customer managed keys

Google Cloud does not support rotating keys on existing persistent disks or images. Once a machine is provisioned it is tied to the key version in use at the time it was created. However, a new version of the key can be created and that new key is used for newly provisioned machines or resources created when a catalog is updated with a new master image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT CONSIDERATIONS ABOUT KEY RINGS

Key rings cannot be renamed or deleted. Also, you might incur unforeseen charges when configuring them. When deleting or removing a key ring, Google Cloud displays an error message:

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

TIP:

For more information, see Editing or deleting a key ring from the console.

Uniform bucket-level access compatibility

Citrix DaaS is compatible with uniform bucket-level access control policy on Google Cloud. This functionality augments the use of IAM policy that grants permissions to a service account to allow for the manipulation of resources, including storage buckets. With uniform bucket level access control, Citrix DaaS allows you to use an access control list (ACL) to control access to storage buckets or objects stored in them. See Uniform bucket-level access for overview information about Google Cloud uniform bucket-level access. For configuration information, see Require uniform bucket-level access.

Use PowerShell

This section details how to do the following tasks using PowerShell:

- Create a catalog with persistent write-back cache disk
- Improve boot performance with MCSIO
- Create a catalog with CMEK using custom properties

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Create a machine catalog using a machine profile
- Create a machine catalog with machine profile as an instance template
- Create a catalog with shielded VM
- Create Windows 11 VMs on the sole-tenant node
- VMs and disks with inherited labels

Create a catalog with persistent write-back cache disk

To configure a catalog with persistent write-back cache disk, use the PowerShell command `New-ProvScheme CustomProperties`.

TIP:

Use the PowerShell parameter `New-ProvScheme CustomProperties` only for cloud-based hosting connections. If you want to provision machines using a persistent write-back cache disk for an on-premises solution (for example, XenServer®) PowerShell is not needed because the disk persists automatically.

This command supports an extra property, `PersistWBC`, used to determine how the write-back cache disk persists for MCS provisioned machines. The `PersistWBC` property is only used when the `UseWriteBackCache` parameter is specified, and when the `WriteBackCacheDiskSize` parameter is set to indicate that a disk is created.

NOTE:

This behavior applies to both Azure and GCP where the default MCSIO write-back cache disk is deleted and re-created when power cycling. You can choose to persist the disk to avoid the deletion and recreation of MCSIO write-back cache disk.

Examples of properties found in the `CustomProperties` parameter before supporting `PersistWBC` include:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

NOTE:

This example only applies to Azure. The properties are different in GCP environment.

When using these properties, consider that they contain default values if the properties are omitted from the `CustomProperties` parameter. The `PersistWBC` property has two possible values: **true** or **false**.

Setting the `PersistWBC` property to **true** does not delete the write-back cache disk when the Citrix DaaS administrator shuts down the machine from the management interface.

Setting the `PersistWBC` property to **false** deletes the write-back cache disk when the Citrix DaaS administrator shuts down the machine from the management interface.

NOTE:

If the `PersistWBC` property is omitted, the property defaults to **false** and the write-back cache is deleted when the machine is shut down from the management interface.

For example, using the `CustomProperties` parameter to set `PersistWBC` to true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</CustomProperties>
```

IMPORTANT:

The `PersistWBC` property can only be set using the `New-ProvScheme` PowerShell cmdlet. Attempting to alter the `CustomProperties` of a provisioning scheme after creation has no impact on the machine catalog and the persistence of the write-back cache disk when a machine is shut down.

For example, set `New-ProvScheme` to use the write-back cache while setting the `PersistWBC` property to true:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Improve boot performance with MCSIO

You can improve boot performance for Azure and GCP managed disks when MCSIO is enabled. Use the PowerShell `PersistOSDisk` custom property in the `New-ProvScheme` command to configure this feature. Options associated with `New-ProvScheme` include:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource``````````````Groups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

To enable this feature, set the `PersistOSDisk` custom property to **true**. For example:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Create a catalog with CMEK using custom properties

When creating your Provisioning Scheme via PowerShell, specify a `CryptoKeyId` property in `ProvScheme CustomProperties`. For example:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

The `cryptoKeyId` must be specified in the following format:

`projectId:location:keyRingName:cryptoKeyName`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, if you'd like to use the key `my-example-key` in key ring `my-example-key-ring` in the region `us-east1` and project with ID `my-example-project-1`, your `ProvScheme` custom settings would resemble:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

All MCS provisioned disks and images related to this provisioning scheme use this customer managed encryption key.

TIP:

If you use global keys, the customer properties location must say `global` and not the **region** name, which in the example above is **us-east1**. For example: `<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`.

Create a machine catalog using a machine profile

When you create a catalog to provision machines using Machine Creation Services (MCS), you can use a machine profile to capture the hardware properties from a virtual machine and apply them to newly provisioned VMs in the catalog. When `MachineProfile` parameter is not used, the hardware properties are captured from the master image VM or snapshot. Some properties you define explicitly, for example, `StorageType`, `CatalogZones` and `CryptoKeyId` are ignored from machine profile.

- To create a catalog with a machine profile, use the `New-ProvScheme` command. For example, `New-ProvScheme –MachineProfile “path to VM”`. If you do not specify the `MachineProfile` parameter, hardware properties are captured from the master image VM.
- To update a catalog with a new machine profile, use the `Set-ProvScheme` command. For example, `Set-ProvScheme –MachineProfile “path to new VM”`. This command does not change the machine profile of the existing VMs in the catalog. Only the newly created VMs added to the catalog have the new machine profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can also update the master image, however, when you update the master image, the hardware properties are not updated. If you want to update the hardware properties, you need to update the machine profile using `Set-ProvScheme` command. These changes will only apply to the new machines in the catalog. For updating the hardware properties of an existing machine, you can use the command `Set-ProvVMUpdateTimeWindow` with `-StartsNow` and `-DurationInMinutes -1` parameters.

  NOTE:

  - `StartsNow` indicates that the scheduled start time is the current time.
  - `DurationInMinutes` with a negative number (for example, –1) indicates no upper bound on the schedule's time window.

Create a machine catalog with machine profile as an instance template

You can select a GCP instance template as an input for the machine profile. Instance templates are lightweight resources in GCP, therefore, are very cost effective.

Create a new machine catalog with machine profile as an instance template

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Find an instance template in your GCP project using the following command:

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. Create a new machine catalog with machine profile as an instance template using NewProvScheme command:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName>\Base.vm\Base.snapshot
-MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on the New-ProvScheme command, see `<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/>`.

5. Finish creating the machine catalog using PowerShell commands.

Update a machine catalog to have an instance template as machine profile

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run the following command:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

For information on the Set-ProvScheme command, see `<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/>`.

Create a catalog with shielded VM

You can create an MCS machine catalog with shielded VM properties. A shielded virtual machine is hardened by a set of security controls that provide verifiable integrity of your Compute Engine instances, using advanced platform security capabilities like secure boot, a virtual trusted platform module, UEFI firmware and integrity monitoring.

MCS supports creating the catalog using the machine profile workflow. If you use machine profile workflow, then you must enable the shielded VM properties of a VM instance. You can then use this VM instance as a machine profile input.

Create an MCS machine catalog with shielded VM

1. Enable shielded VM options of a VM instance in Google Cloud console. See Quickstart: Enable Shielded VM options.
2. Create an MCS machine catalog with machine profile workflow by using the VM instance.
    a. Open a PowerShell window
    b. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
    c. Create an identity pool if not already created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Run the `New-ProvScheme` command. For example:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>

-HostingUnitName gcp-hostint-unit

-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm

-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
machine.vm
```

3. Finish creating the machine catalog.

Update a machine catalog with a new machine profile

1. Run the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>

-MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

-MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
```

To apply the change done in `Set-ProvScheme` to the existing VMs, run the `Set-ProvVMUpdateTimeWindow` command.

1. Run `Set-ProvVMUpdateTimeWindow` command. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. Restart the VMs.

Create Windows 11 VMs on the sole-tenant node

You can create Windows 11 VMs in GCP. However, if you install Windows 11 on the master image, then you must enable vTPM during the master image creation process. Also, you must enable vTPM on the machine profile source (VM or instance template).

The key steps to create Windows 11 VMs on the sole-tenant node are:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Set up the Google Cloud virtualization environments. For information, see Google Cloud environments.
2. Install VDA. See Install VDAs.
3. Create a connection to Google cloud environments. For information, see Connection to Google cloud environments.
4. Create a Windows 11 Bring Your Own License (BYOL) master image and import the image to Google Cloud. See Create a Windows 11 BYOL master image.
5. Create the machine profile source: Provision VM on the sole-tenant node and enable the vTPM of the source machine profile. See Provision VM on sole-tenant node.
6. Create an MCS machine catalog using the Windows 11 machine profile source enabled with vTPM. The machine profile source must have the same instance type as described in the sole-tenant node. See Create an MCS machine catalog using the Windows 11 machine profile source.

Create a Windows 11 BYOL master image

There are two option to create a Windows 11 BYOL master image and import the master image to Google Cloud:

- Use Google Cloud Cloud Build Tools
- Create the master image on any other hypervisor

USE GOOGLE CLOUD CLOUD BUILD TOOLS

1. Upload the Windows 11 ISO, GCP SDK, .NET framework and PowerShell installer files to the GCP storage bucket.
2. Provide the file location in the cloud build `.yaml` file as parameter.
3. Run the following Cloud Build from the command line to build the final Windows 11 image. GCP bootstraps and creates the master image in the selected project using Daisy workflow in GCP and the master image is imported into GCP.

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

NOTE:

Replace all the capital letter text with the actual resource details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For the complete information, see Create custom Windows BYOL images.

CREATE THE MASTER IMAGE ON ANY OTHER HYPERVISOR

1. Create the Windows 11 master image using any other hypervisor.
2. Export the master image in an OVF format to the local machine.
3. Upload the OVF files to the GCP storage bucket using the local gcloud CLI.

   ```
   gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
   ```

4. Run the following Cloud Build from the command line to build the final Windows 11 image. GCP bootstraps and creates the master image in the selected project using Daisy workflow in GCP and the master image is imported into GCP.

   ```
   gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
   IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
   machine-type=MACHINE-TYPE --zone=ZONE
   ```

   NOTE:

   Replace all the capital letter text with the actual resource details.

Provision VM on sole-tenant node

Use sole-tenant nodes to keep your VMs physically separated from VMs in other projects, or to group your VMs together on the same host hardware. For information on the sole-tenant node, see the GCP document Sole-tenancy overview.

For provisioning a VM (machine profile source) on the sole-tenant node, see the GCP document Provision VMs on sole-tenant nodes.

NOTE:

- Select the same Instance type and region as the node group.
- Enable vTPM in the Shielded VM section. For more information, see Quickstart: Enable Shielded VM options.
- Disable the Bitlocker on the source VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create an MCS machine catalog using the Windows 11 machine profile source

You can create an MCS machine catalog to create Windows 11 VMs using Studio or PowerShell commands.

NOTE:

- For the master image, select the Windows 11 Snapshot or VM.
- For the machine profile source, select the Windows 11 VM as machine profile. The machine profile source must have the same instance type as described in the sole-tenant node.

For information on using Studio, see Create a machine catalog using Studio.

For information on PowerShell commands, see Create a machine catalog using a machine profile.

After you create the catalog and power on the VMs, you can see the Windows 11 VMs running on the sole tenant node on the Google Cloud console.

VMs and disks with inherited labels

MCS machine catalog VMs and disks (Identity Disk, Write-cache Back Disk, and OS disk) can inherit the labels of a machine profile source (GCP VM instance or instance template). You can use the labels to distinguish instances owned by different teams (for example, team:research and team:analytics), and further use it for cost accounting or budgeting. For more information on labels, see the GCP document Organize resources using labels.

You can create a new catalog, update an existing catalog, and update existing VMs to inherit the labels using the machine profile source.

This feature is applicable to persistent and non-persistent MCS machine catalogs.

You can do the following:

- Create a catalog with inherited labels
- Update an existing catalog with inherited labels
- Update existing VMs with inherited labels
- Retrieve information for VM and boot disk labels
- Remove a VM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a catalog with inherited labels

To create an MCS machine catalog where VMs and disk inherit labels from the machine profile source, do the following:

1. Create a machine profile source (VM instance or instance template) with labels. For information on creating VMs with labels, see the GCP document Create resources with labels. An Instance template is created from the VM and takes the labels defined in the VM.
2. Create an MCS catalog using Studio or PowerShell commands.
3. If using Studio, on the **Image** page, select **Use a machine profile**, and then select the VM or template.
4. If using PowerShell commands, do the following:

    a. Open the PowerShell window.

    b. Run asnp citrix*.

    c. Create an identity pool. The identity pool is a container for the Active Directory (AD) accounts for the VMs to be created.

    d. Create the required AD computer accounts in Active Directory.

    e. Run the `New-ProvScheme` command to create a catalog. For example:

    New-ProvScheme with template as machine profile input (Persistent catalog):

    ```
    New-ProvScheme `

    -ProvisioningSchemeName "catalog-name" `

    -HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

    -IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

    -MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

    -MachineProfile "XDHyp:\HostingUnits\hosting-unit-
    name\instanceTemplates.folder\instance-template-name.template" `
    ```

    New-ProvScheme with instance template as machine profile input (Non-Persistent catalog):

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `

-CleanOnBoot
```

New-ProvScheme with VM instance as machine profile input (Persistent catalog):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

New-ProvScheme with VM instance as machine profile input (Non-Persistent catalog):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-CleanOnBoot
```

f. Register provisioning scheme as a broker catalog.

g. Add VMs to the catalog.

Update an existing catalog with inherited labels

To update an existing catalog to have a new machine profile, run the Set-ProvScheme command. After you run the command, all the new VMs added to the catalog have the labels of the new machine profile source. The non-persistent catalog is updated on the next power on.

For example:

Set-ProvScheme with instance template as machine profile input:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

Set-ProvScheme with VM instance as machine profile input:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

Update existing VMs with inherited labels

To update existing VMs with the updated machine profile source, run the following commands:

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

3. Restart the VMs.

Retrieve information for VM and boot disk labels

After creating the VMs, you can get the information of the VM and boot disk label using the `Get-Item` command with the `AdditionalData` parameter.

For retrieving information of the VM label, run the following command:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-
name\vm_name.vm).AdditionalData.Tags
```

For retrieving information of the boot disk label, run the following command:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
name.attacheddisk).AdditionalData.Tags
```

NOTE:

To maintain consistency across the various hypervisors, we have used the term Tags to display GCP labels.

Remove a VM

You can choose to remove a VM from a catalog but not delete the VM from the GCP. In this case, the Citrix labels are only removed from the VM. All other added labels are not deleted from the VM. You can remove a VM from Studio or use PowerShell commands.

USING STUDIO

1. Select and right-click the VM.
2. Click **Delete**.
3. Select **Remove the virtual machines from the catalog but do not delete the virtual machines**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USING POWERSHELL COMMANDS

Run `Remove-ProvVM` with `ForgetVM` parameter. For more information, see the SDK doc Remove-ProvVM.

Google Cloud Marketplace

You can browse and select images offered by Citrix on Google Cloud Marketplace to create machine catalogs. Currently, MCS supports only the machine profile workflow for this feature.

To search for Citrix VDA VM product through Google Cloud Marketplace, go to `<https://console.cloud.google.com/marketplace/>`.

You can use a custom image or a Citrix ready® image on Google Cloud Marketplace to update an image of a machine catalog.

NOTE:

If the machine profile does not contain storage type information, the value is derived from custom properties.

The supported Google Cloud Marketplace images are:

- Windows 2019 Single Session
- Windows 2019 Multi Session
- Ubuntu

Example of using a Citrix ready image as a source for creating a machine catalog:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To manage catalogs, see Manage machine catalogs and Manage a Google Cloud Platform catalog.

More information

- Create and manage connections and resources
- Connection to Google cloud environments
- Create machine catalogs

Create an HPE Moonshot machine catalog

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to HPE Moonshot environments.

NOTE:

- Create a connection to HPE Moonshot
- Make sure to have one or more HPE Moonshot nodes available and install VDAs on those nodes.
- For information about creating the initial HPE Moonshot cartridge image, see the OS Deployment on Moonshot User Guide.

You can create an HPE Moonshot machine catalog using:

- Studio
- PowerShell commands

Create a machine catalog using Studio

In the **Machine Catalog Setup** wizard:

1. On the **Operating System** page, select **Multi-session OS** or **Single-session OS**.
2. On the **Machine Management** page, select **Machines that are power managed** and **Another service or technology**.
3. On the **Virtual Machines** page, add machines and their Active Directory machine accounts. You can do either of the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Click **Add Machines** to add machines manually. The **Select VMs** window appears. Expand the HPE Moonshot chassis connection you created earlier and select the nodes (VMs) you want to add. Then add the associated machine account names.
- Click **Add CSV File** to bulk add machines. For information about using CSV files to add machines, see Use CSV files to bulk add machines to a catalog.

The **Scopes** and **Summary** pages do not contain HPE Moonshot-specific information.

Create a machine catalog using PowerShell commands

Run the `New-BrokerCatalog` and `New-BrokerMachine` PowerShell commands to create a broker catalog and import machines to the broker catalog.

For example:

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage an HPE Moonshot catalog.

More information

- Create and manage connections and resources
- Connection to HPE Moonshot
- Create machine catalogs

Create a Microsoft Azure catalog

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Microsoft Azure Resource Manager cloud environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Before creating a Microsoft Azure catalog, you need to finish creating a connection to Microsoft Azure. See Connection to Microsoft Azure.

Create a machine catalog

You can create a machine catalog in two ways:

- Studio.
- PowerShell. See Manage Citrix DaaS using Remote PowerShell SDKs. For information on how to implement specific features using PowerShell, see Use PowerShell.

Create a machine catalog using an Azure Resource Manager image in Studio

This information is a supplement to the guidance in Create machine catalogs.

An image can be a disk, snapshot, or an image version of an image definition inside the Azure Compute Gallery that is used to create the VMs in a machine catalog.

Before creating the machine catalog, create an image in Azure Resource Manager.

NOTE:

- Use of unmanaged disk to provision VM is deprecated.
- Support for using a master image from a region different from that configured in the host connection is deprecated. Use Azure Compute Gallery to replicate the master image to the desired region.

When creating an MCS machine catalog, a temporary VM is created based on the original VM to perform preparation tasks such as enabling DHCP and license rearm. This temporary VM is called a preparation VM. The name of this preparation VM follows the format **Preparati-84x9n**, where the last five characters are randomly generated to avoid duplication. The naming convention for this preparation VM is fixed and cannot be customized. After the preparation tasks are completed, the preparation VM is destroyed.

To disconnect the network from the preparation VM, a network security group is created to deny all inbound and outbound traffic. The network security group is created automatically once per catalog. The network security group's name is `Citrix-Deny-All-a3pgu-GUID`, where GUID is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

randomly generated. For example, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

In the machine catalog creation wizard:

1. The **Machine Type** and **Machine Management** pages do not contain Azure-specific information. Follow the guidance in the Create machine catalogs article.
2. On the **Image** page, select an image that you want to use as the master image for all machines in the catalog. The **Select an image** wizard appears. Follow these steps to select an image:

   a. (Applicable only to connections configured with shared images within or across tenants) Select a subscription where the image resides.

   b. Select a resource group.

   c. Navigate to the Azure managed disk, Azure Compute Gallery, or Azure image version.

   When selecting an image, consider the following:

   - Verify that a Citrix VDA is installed on the image.
   - If you select a disk attached to a VM, you must shut down the VM before proceeding to the next step.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- The subscription corresponding to the connection (host) that created the machines in the catalog is denoted with a green dot. The other subscriptions are those that have the Azure Compute Gallery shared with that subscription. In those subscriptions, only shared galleries are shown. For information about how to configure shared subscriptions, see Share images within a tenant (across subscriptions) and Share images across tenants.
- You can create a provisioning scheme using ephemeral OS disk on Windows with Trusted Launch. When you select an image with Trusted Launch, then you must select a machine profile with Trusted Launch that is enabled with vTPM. To create machine catalogs using ephemeral OS disk, see How to create machines using ephemeral OS disks.
- When image replication is in progress, you can proceed and select the image as the master image and complete the setup. However, catalog creation might take longer to complete while the image is being replicated. MCS requires the replication to complete within an hour starting from catalog creation. If the replication times out, catalog creation fails. You can verify the replication status in Azure. Try again if the replication is still pending or after the replication completes.
- You can provision a Gen2 VM catalog by using a Gen2 image to improve boot time performance. However, creating a Gen2 machine catalog using a Gen1 image is not supported. Similarly, creating a Gen1 machine catalog using a Gen2 image is also not supported. Also, any older image that does not have generation information is a Gen1 image.

Choose whether you want VMs in the catalog to inherit configurations from a machine profile. By default, the **Use a machine profile (mandatory for Microsoft Entra ID)** checkbox is selected. Click **Select a machine profile** to browse to a VM or an ARM template spec from a list of resource groups.

Examples of configurations that VMs can inherit from a machine profile include:

- Accelerated networking
- Boot diagnostics
- Host disk caching (relating to OS and MCSIO disks)
- Machine size (unless otherwise specified)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Tags placed on the VM

NOTE:

- When you select a master image for machine catalogs in Azure, the machine profile is filtered based on the master image you selected. For example, the machine profile is filtered based on the Windows OS, security type, hibernation support, and disk encryption set ID of the master image.
- Using a machine profile with Trusted Launch as **Security Type** is mandatory when you select an image or snapshot that has Trusted Launch enabled. You can then enable or disable SecureBoot and vTPM by specifying their values in the Machine Profile. For information about Azure Trusted Launch, see `<https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch>`.

Validate the ARM template spec to make sure whether it can be used as a machine profile to create a machine catalog. For information on creating an Azure template spec, see Create an Azure template spec.

There are two ways to validate the ARM template spec:

- After you select the ARM template spec from the resource group list, click **Next**. Error messages appear if the ARM template spec has errors.
- Run one of the following PowerShell commands:
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

  For example:

```
Test-ProvInventoryItem -HostingUnitName "we-vdi0101-d-vnet"
-InventoryPath machineprofile.folder/vdi01-d-rg.resourcegroup/VDD-
templ-spec.templatespec/1.5.templatespecversion
```

After you create the catalog, you can view the configurations that the image inherits from the machine profile. On the **Machine Catalogs** node, select the catalog to view its details in the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

lower pane. Then, click the **Template Properties** tab to view machine profile properties. The **Tags** section displays up to three tags. To view all tags placed on the VM, click **View all**.

If you want MCS to provision VMs on an Azure dedicated host, enable the **Use a host group** checkbox and then select a host group from the list. A host group is a resource that represents a collection of dedicated hosts. A dedicated host is a service that provides physical servers that host one or more virtual machines. Your server is dedicated to your Azure subscription, not shared with other subscribers. When you use a dedicated host, Azure ensures that your VMs are the only machines running on that host. This feature is suitable for scenarios where you must meet regulatory or internal security requirements. To learn more about host groups and considerations for using them, see Provision VMs on Azure dedicated hosts.

IMPORTANT:

- Only host groups that have Azure auto-placement enabled are shown.
- Using a host group changes the **Virtual Machines** page offered later in the wizard. Only machine sizes that the selected host group contains are shown on that page. Also, Availability Zones are selected automatically and not available for selection.

3. The **Storage and License Types** page appears only when you use an Azure Resource Manager image.

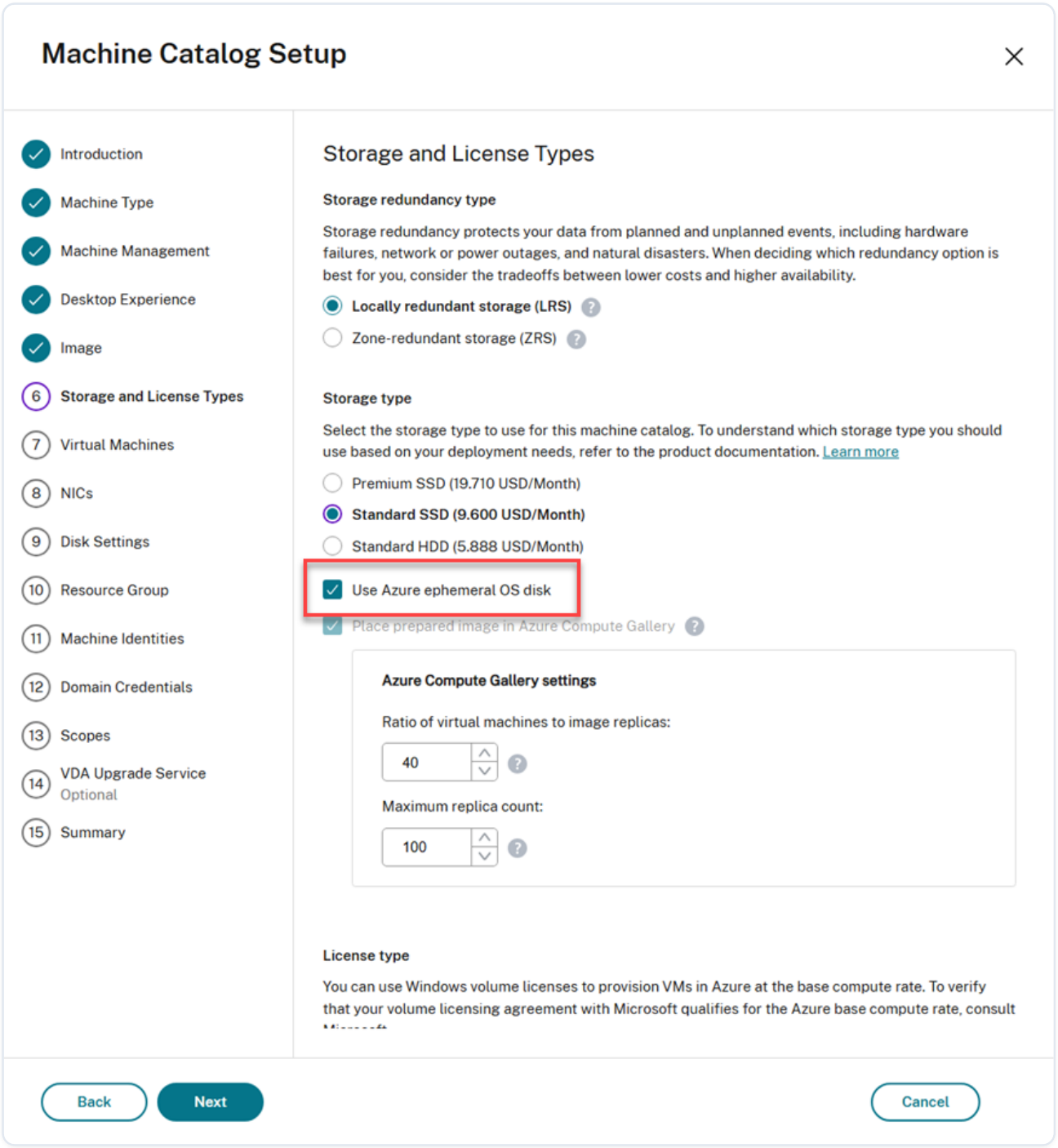
   - Select the **Storage redundancy type**:
     - Local redundant storage (LRS): LRS allows you to choose from all available storage types. When using LRS, Azure deploys the Virtual Machines (VMs) exclusively within the specified availability zone.
     - Zone redundant storage (ZRS): ZRS allows for greater flexibility in VM placement, as Azure can launch VMs in any available zone. This is a key advantage over Local Redundant Storage (LRS), ensuring VM availability even if the disk's original zone becomes inaccessible. ZRS, however, is only compatible with Premium SSD and Standard SSD storage types.
   - Select the **Storage types** to use for the machine catalog: The storage type determines which machine sizes are offered on the **Virtual Machines** page of the wizard.
     - **Premium SSD**. Offers a high-performance, low-latency disk storage option suitable for VMs with I/O-intensive workloads.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **Standard SSD**. Offers a cost-effective storage option that is suitable for workloads that require consistent performance at lower IOPS levels.
  - **Standard HDD**. Offers a reliable, low-cost disk storage option suitable for VMs that run latency-insensitive workloads.

- Select the **Use Azure ephemeral OS disk**. Azure ephemeral OS disk offers a cost-effective storage option that reuses the local disk of the VMs to host the operating system disk. Alternatively, you can use PowerShell to create machines that use ephemeral OS disks. For more information, see Azure ephemeral disks. Consider the following when using an ephemeral OS disk:
  - Azure ephemeral OS disk and MCS I/O cannot be enabled at the same time.
  - To update machines that use ephemeral OS disks, you must select an image whose size does not exceed the size of the VM's cache disk or temporary disk.
  - You cannot use the **Retain VM and system disk during power cycles** option offered later in the wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

- The identity disk is always created using Standard SSD irrespective of the storage type that you choose.
- If you select **ZRS** as the **Storage redundancy**, you get the option to only select **Premium SSD** and **Standard SSD**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For details about Azure storage types and storage replication, see the following:

- [Introduction to Azure Storage](https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/)
- [Azure premium storage: Design for high performance](https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/)
- [Azure Storage redundancy](https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/)

Select whether to use existing Windows licenses or Linux licenses:

- Windows licenses: Using Windows licenses along with Windows images (Azure platform support images or custom images) lets you run Windows VMs in Azure at a reduced cost. There are two types of licenses:

    - **Windows Server license**. Lets you use your Windows Server or Azure Windows Server licenses, allowing you to use Azure Hybrid Benefits. For details, see `<https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>`. Azure Hybrid Benefit reduces the cost of running VMs in Azure to the base compute rate, waiving the cost of extra Windows Server licenses from the Azure gallery.

    - **Windows Client license**. Lets you bring your Windows 10 and Windows 11 licenses to Azure, allowing you to run Windows 10 and Windows 11 VMs in Azure without the need for extra licenses. For details, see [Client Access Licenses and Management Licenses](https://www.microsoft.com/en-us/licensing/product-licensing/client-access-license).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Linux licenses: With bring-your-own-subscription (BYOS) Linux licenses, you do not have to pay for the software. The BYOS charge only includes the compute hardware fee. There are two types of licenses:

    - **RHEL_BYOS**: To use RHEL_BYOS type successfully, enable Red Hat Cloud Access on your Azure subscription.

    - **SLES_BYOS**: The BYOS versions of SLES include support from SUSE.

See the following:

- [Verify the Windows license](#verify-the-windows-license)

- [Configure the Linux license](#configure-the-linux-license)

See the following documents to understand License types and their benefits:

- `<https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`

- `<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

Azure Compute Gallery is a repository for managing and sharing images. It lets you make your images available throughout your organization. We recommend that you store an image in Azure Compute Gallery when creating

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
large non-persistent machine catalogs because doing that enables faster
resets of VDA OS disks. After you select **Place prepared image in Azure
Compute Gallery**, the **Azure Compute Gallery settings** section appears,
letting you specify more Azure Computer Gallery settings:



-  **Ratio of virtual machines to image replicas**. Lets you specify the
ratio of virtual machines to image replicas that you want Azure to keep.
By default, Azure keeps a single image replica for every 40 non-persistent
machines. For persistent machines, that number defaults to 1,000.



-  **Maximum replica count**. Lets you specify the maximum number of image
replicas that you want Azure to keep. The default is 100.



For information on Azure Compute Gallery, see [Azure Compute Gallery]
(#azure-compute-gallery).



> **Note:**

>

> A gallery is created in ACG to store the image. This gallery is
accessible only to MCS for VM creation and doesn't appear on the **Select
an image** page.
```

1. On the **Virtual Machines** page, indicate how many VMs you want to create and the machine size. After catalog creation, you can change the machine size by editing the catalog.

   You can now configure a secondary VM when the primary machine size reaches full capacity. To configure secondary VM sizes, click **Secondary size (optional)**.

   a. In the **Secondary machine size** window, the VMs listed have both, Spot and Regular VM types. You may select up to 10 secondary machines sizes. Once the 10 VMs are selected, then the other VMs listed are disabled from further selection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Click **Next**. In the **Secondary machine size** blade, you can select multiple machine sizes and drag and drop to change the priority order. Click **Done**. The selected machine sizes show up in the **Secondary size (optional)**. Click the edit icon to edit as needed.

NOTE:

- If the Temporary Disk Size property is set for a primary VM then, only the secondary VMs with Temporary Disk Size property set are listed.
- If the Temporary Disk Size property is not set for a primary VM then, the secondary VMs without Temporary Disk Size property are listed.
- If you modify the primary VM, you must re-configure the secondary VM.
- Machine profiles are mandatory for secondary machine sizes.
- The secondary VM sizes which do not support spot are shown only when one of the following condition is matched; otherwise, all secondary VM sizes are shown:
- The primary VM size does not support spot
- The primary VM size supports spot but MP does not support spot
- The machine profile supports hibernation

2. The **NICs** page does not contain Azure-specific information. Follow the guidance in the Create machine catalogs article.
3. On the **Disk Settings** page, choose whether to enable write-back cache. With the MCS storage optimization feature enabled, you can configure the following settings when creating a catalog.

   After enabling write-back cache, you can do the following:

   - Configure the size of the disk and RAM used for caching temporary data. For more information, see Configure cache for temporary data.
   - Select the storage type for the write-back cache disk. The following storage options are available to use for the write-back cache disk:
     - Premium SSD
     - Standard SSD
     - Standard HDD

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> If you select **ZRS** as **Storage redundancy** on the **Storage and License Types** page, then write-back cache disk storage redundancy is set as ZRS by default.

- Choose whether you want the write-back cache disk to persist for the provisioned VMs. Select **Enable write-back cache** to make the options available. By default, **Use non-persistent write-back cache disk** is selected.
- Select the type for the write-back cache disk.
  - **Use non-persistent write-back cache disk**. If selected, the write-back cache disk is deleted during power cycles. Any data redirected to it will be lost. If the VM's temporary disk has sufficient space, it is used to host the write-back cache disk to reduce your costs. After catalog creation, you can check whether the provisioned machines use the temporary disk. To do so, click the catalog and verify the information on the **Template Properties** tab. If the temporary disk is used, you see **Non-persistent Write-back Cache Disk** and its value is **Yes (using VM's temporary disk)**. If not, you see **Non-persistent Write-back Cache Disk** and its value is **No (not using VM's temporary disk)**.
  - **Use persistent write-back cache disk**. If selected, the write-back cache disk persists for the provisioned VMs. Enabling the option increases your storage costs.

> **NOTE:**
>
> A catalog automatically uses Azure Temp Disk for WBC disk if all the following criteria are met:

  - MCSIO is enabled.
  - The WBC disk is non-persistent.
  - The VM size includes a Temp Disk large enough for the WBC disk.
  - No drive letter is specified for the WBC disk. This feature applies to both catalog creation and editing, helping reduce your storage costs.

- Choose whether to retain VMs and system disks for VDAs during power cycles.

  Retain VM and system disk during power cycles. Available when you've selected **Enable write-back cache**. By default, VMs and the system disks are deleted on shutdown

© 1997–2026 Citrix Systems, Inc. All rights reserved.

and recreated on startup. If you want to reduce VM restart times, select this option. Keep in mind that enabling this option also increases storage costs.

- Choose whether to **Enable storage cost saving**. If enabled, save storage costs by downgrading the storage disk to Standard HDD when the VM shuts down. The VM switches to its original settings on restart. The option applies to both storage and write-back cache disks. Alternatively, you can also use PowerShell. See Change the storage type to a lower tier when a VM is shut down.

  NOTE:

  Microsoft imposes restrictions on changing the storage type during VM shutdown. It's also possible that Microsoft will block storage type changes in the future. For more information, see this Microsoft article.

- Choose whether to encrypt data on machines in this catalog and which encryption key to use. Server-side encryption with a customer-managed key (CMK) lets you manage encryption at a managed disk level and protect data on the machines in the catalog. Default settings are inherited from either the machine profile or the master image, with the profile taking priority:

  - If you're using a *machine profile* with a *CMK*, the **Use the following key to encrypt data on each machine** option is auto-selected and defaults to the key from the *machine profile*.
  - If you're using a *machine profile* with a Platform Managed Key (PMK) and the *master image* is *CMK* encrypted, the **Use the following key to encrypt data on each machine** option is auto-selected and defaults to the key from the master image.
  - If you're *not* using a *machine profile* and the *master image* is *CMK* encrypted, the **Use the following key to encrypt data on each machine** option is auto-selected and defaults to the key from the *master image*.

For more information, see Azure server side encryption.

4. On the **Resource Group** page, choose whether to create resource groups or use existing groups.

   - If you choose to create resource groups, select **Next**.
   - If you choose to use existing resource groups, select groups from the **Available Provisioning Resource Groups** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> Select enough groups to accommodate the machines you're creating in the catalog. A message appears if you choose too few. You might want to select more than the minimum required if you plan to add more VMs to the catalog later. You can't add more resource groups to a catalog after the catalog is created.

For more information, see Azure resource groups.

5. On the **Machine Identities** page, choose an identity type and configure identities for machines in this catalog. If you select the VMs as **Microsoft Entra joined**, you can add them to a Microsoft Entra security group. Detailed steps are as follows:

   a. From the **Identity type** field, select **Microsoft Entra joined**.

   b. Click **Select service account** and select a service account with the **Microsoft Entra security group management** capability.

   c. Click **Microsoft Entra security group: Create new**.

   > **NOTE:**
   >
   > **Create new** is dimmed if the selected service account lacks the **Microsoft Entra security group management** capability.

   d. Enter a group name, and then click **Create**.

   e. To add the security group to an assigned security group, select **Join an assigned security group as a member**, and then click **Select a group** to choose an assigned group to join.

   f. Enter the machine account naming scheme for the VMs.

   After catalog creation, Citrix DaaS™ accesses Azure using the service account you selected and creates the security group and a dynamic membership rule for the group. Based on the rule, VMs with the naming scheme specified in this catalog are automatically added to the security group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> To rename the Microsoft Entra security group after catalog creation, edit the catalog and go to **Microsoft Entra Security Group** from the left navigation. Names of Microsoft Entra security groups must not contain the following characters: `@ " \ / ; : # . * ? = < > | [ ] ( ) '`.

6. On the **Domain Credentials** page, follow the guidance in the Create Machine Catalogs article to complete settings.
7. On the **Summary** page, review the settings you specified, and click **Finish**.

> **TIP:**
>
> You can view the estimated monthly cost for the virtual machines in this machine catalog based on Azure's public list price. If the connection hosting the catalog has the `Microsoft.Consumption/pricesheets/read` permission in Azure, the estimate is calculated using your organization's contracted pricing instead.

Select the cost estimate to see detailed information. For a more accurate estimate, adjust settings such as daily power-on hours, workdays per week, and savings options based on your usage.

Create an Azure template spec

You can create an Azure template spec in the Azure portal and use it in Studio and PowerShell commands to create or update an MCS machine catalog.

To create an Azure template spec for an existing VM:

1. Go to the Azure portal. Select a resource group, and then select the VM and network interface. From the **…** menu on the top, click **Export template**.
2. Clear the **Include parameters** checkbox if you want to create a template spec for catalog provisioning. Verify in the JSON file that the `parameters` and `variables` sections are:

```
"parameters": {},

"variables": {}
```

3. Click **Download** to save the template as JSON file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. On the Azure portal, select **Template specs** and click **Import Template**.
5. Browse and import the machine profile (in JSON) saved on your computer.
6. Provide the **Name**, **Subscription**, **Resource Group**, **Location**, and **Version**. Click **Next: Edit Template**.
7. Create **Review+Create** and create the template spec.
8. On the **Template Specs** page, verify the template spec you created. Click the template spec. On the left panel, click **Versions**.
9. You can create a new version by clicking **Create new version**. Specify a new version number, make changes to the current template spec, and click **Review + Create** to create the new version of the template spec.

You can get information about the template spec and template version using the following PowerShell commands:

- To get information about the template spec, run:

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- To get information about the template spec version, run:

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

Use a template spec in creating or updating a catalog

You can create or update an MCS machine catalog using a template spec as a machine profile input. To do this, you can:

- Use Studio. See Create a machine catalog using an Azure Resource Manager image in Studio.
- Use PowerShell. See Use template spec in creating or updating a catalog using PowerShell

Export a machine profile to a JSON file

You can export the machine profile used by a catalog into a JSON file. This function enables you to customize the profile and import it into Azure as an ARM Template spec for future provisioning.

1. On the **Machine Catalogs** page, select a machine catalog to view details in the lower pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click the **Template Properties** tab to view machine profile properties and click **Export**.
3. Specify a path on your local computer to save the machine profile as a JSON file.

Import a machine profile as an ARM Template spec in Azure

1. On the Azure portal, select **Template specs** and click **Import Template**.
2. Browse and import the machine profile (in JSON) saved on your computer.
3. Provide the **Name**, **Subscription**, **Resource Group**, **Location**, and **Version** for the importing template and click **Review + Create**. The template is validated and imported successfully. The imported template is listed in the **Template specs**.

When you create machine catalogs using machine profiles, you can see this template when choosing profiles. For more information, see Use a template spec in creating or updating a catalog.

Provision machines into specified Availability Zones

You can provision machines into specific Availability Zones in Azure environments. You can achieve that using Studio or PowerShell.

NOTE:

- If no zones are specified, MCS lets Azure place the machines within the region. If more than one zone is specified, MCS randomly distributes the machines across them.
- If you select ZRS as Storage redundancy on the Storage and License Types page, then you get a warning suggesting to clear the zone selection and let Azure manage the VM availability zones. You get the warning only if you select a machine profile or host group that has availability zones.

Configure Availability Zones in Studio

When creating a machine catalog, you can specify Availability Zones into which you want to provision machines. On the **Virtual Machines** page, select one or more Availability Zones where you want to create machines.

There are two reasons that no Availability Zones are available: The region has no Availability Zones or the selected machine size is unavailable.

For information on configuring using PowerShell command, see Configure Availability Zones using PowerShell.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure ephemeral disks

An Azure ephemeral disk allows you to repurpose the cache disk, temporary disk, or NVMe disk to store the OS disk for an Azure-enabled virtual machine. This functionality is useful for Azure environments that require a higher performant SSD disk over a standard HDD disk. For information on creating a catalog with an Azure ephemeral disk, see Create a catalog with an Azure ephemeral disk.

NOTE:

Persistent catalogs do not support ephemeral OS disks.

Ephemeral OS disks require that your provisioning scheme use managed disks and an Azure Compute Gallery. For more information, see Azure shared image gallery.

Store an ephemeral OS temporary disk

You have the option of storing an ephemeral OS disk on the VM temp disk, a resource disk, or an NVMe disk. This functionality enables you to use an ephemeral OS disk with a VM that either doesn't have a cache, or has insufficient cache. Such VMs have a temp disk, resource disk, or NVMe disk to store an ephemeral OS disk, such as `Ddv4`.

Consider the following:

- An ephemeral disk is stored either in the VM cache disk, or the VMs temporary (resource) disk or the NVMe disk. The cache disk is preferred over the temporary disk, unless the cache disk is not large enough to hold the contents of the OS disk.
- For updates, a new image that is larger than the cache disk but smaller than the temp disk results in replacing the ephemeral OS disk with the VM's temp disk.

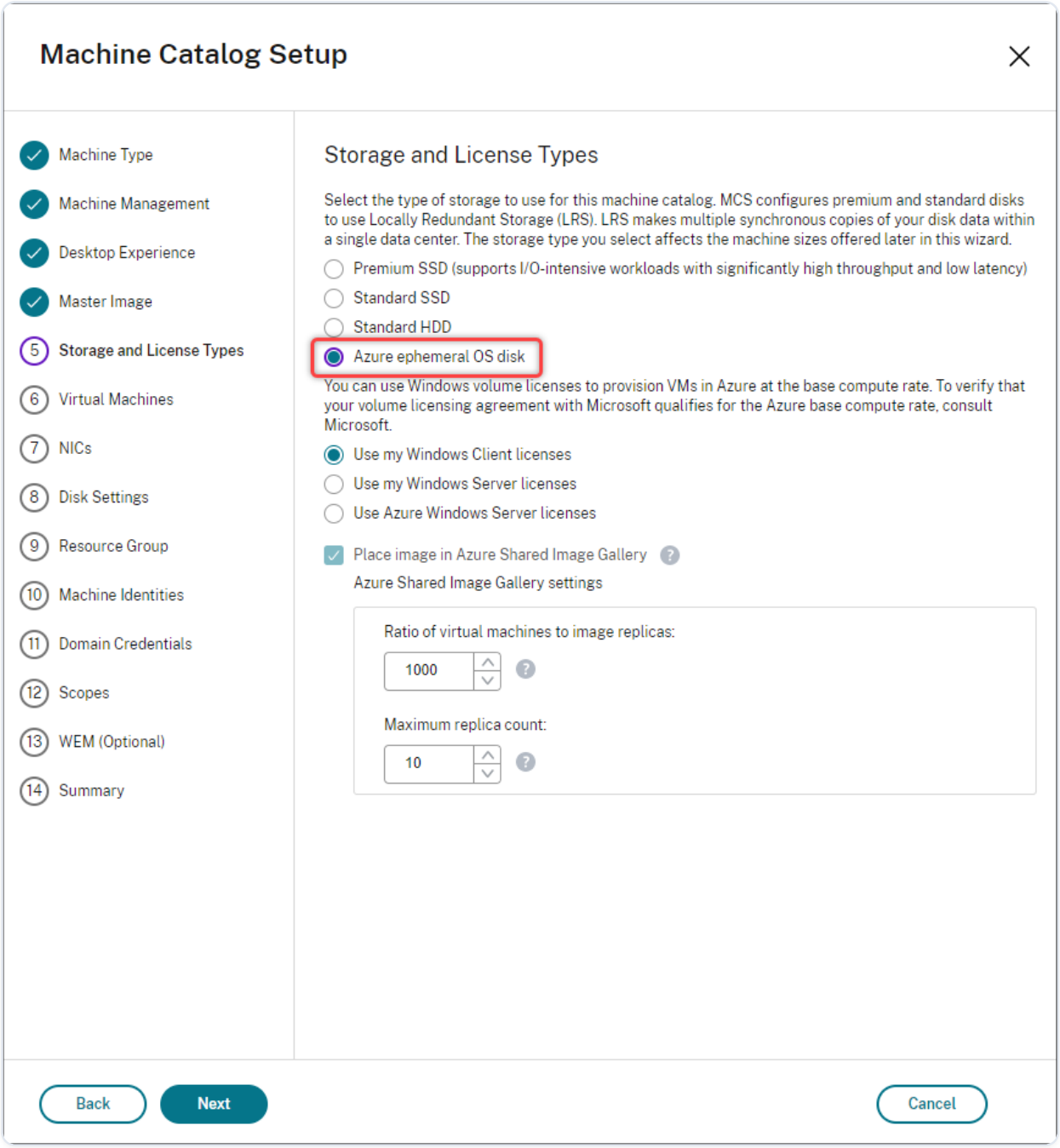
Azure ephemeral disk and Machine Creation Services (MCS) storage optimization (MCS I/O)

Azure ephemeral OS disk and MCS I/O cannot be enabled at the same time.

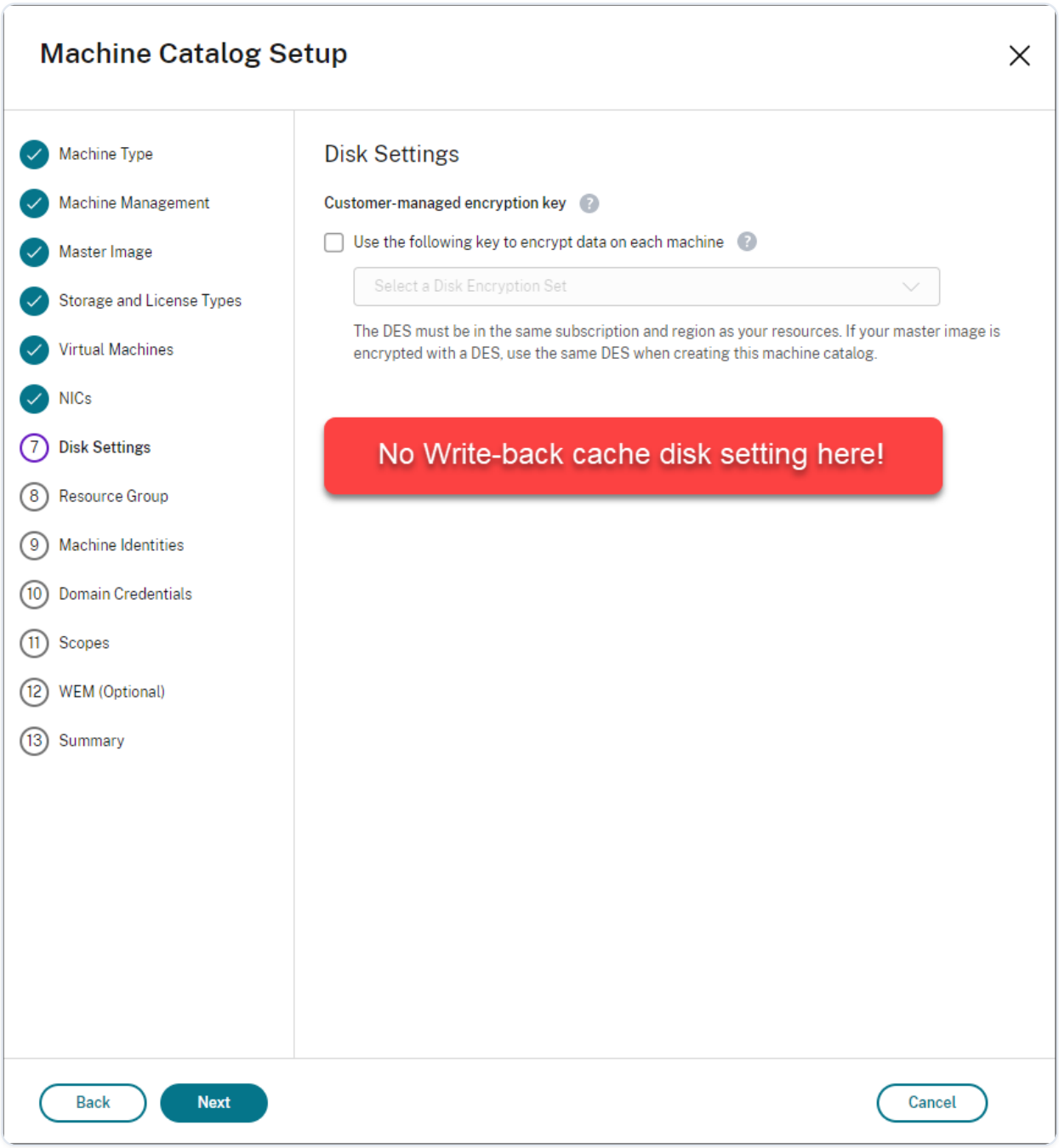
The important considerations are as follows:

- You cannot create a machine catalog with both ephemeral OS disk and MCS I/O enabled at the same time.
- In the **Machine Catalog Setup** wizard, if you select **Azure ephemeral OS disk** on the **Storage and License Types** page, you do not get the option for write-back cache disk settings on the **Disk Settings** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The PowerShell parameters (`UseWriteBackCache` and `UseEphemeralOsDisk`) set to **true** in `New-ProvScheme` or `Set-ProvScheme` fails with proper error message.
- For existing machine catalogs created with both features enabled, you can still:
  - update a machine catalog.
  - add or delete VMs.
  - delete a machine catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure Compute Gallery

Use Azure Compute Gallery (formerly Shared Image Gallery) as a published image repository for MCS provisioned machines in Azure. You can store a published image in the gallery to accelerate the creation and hydration of OS disks, improving start and application launch times for non-persistent VMs. Azure Compute Gallery contains the following three elements:

- Gallery: Images are stored here. MCS creates one gallery for each machine catalog.
- Gallery Image Definition: This definition includes information (operating system type and state, Azure region) about the published image. MCS creates one image definition for each image created for the catalog.
- Gallery Image Version: Each image in an Azure Compute Gallery can have multiple versions, and each version can have multiple replicas in different regions. Each replica is a full copy of the published image. Citrix DaaS creates one Standard_LRS image version (version 1.0.0) for each image with the appropriate number of replicas in the catalog's region, based on the number of machines in the catalog, the configured replica ratio, and the configured replica maximum.

NOTE:

Azure Compute Gallery functionality is only compatible with managed disks. It is not available for legacy machine catalogs.

For more information, see Azure shared image gallery overview.

Access images from Azure Compute Gallery

When selecting an image to use for creating a machine catalog, you can select images you created in the Azure Compute Gallery. These images appear in the list of images on the **Image** page of the Machine Catalog Setup wizard.

For these images to appear, you must:

1. Set up Citrix DaaS.
2. Connect to the Azure Resource Manager.
3. In the Azure portal, create a resource group. For details, see Create an Azure Shared Image Gallery using the portal.
4. In the resource group, create an Azure Compute Gallery.
5. In the Azure Compute Gallery, create an image definition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. In the image definition, create an image version.

For information on configuring the Azure Compute Gallery, see Configure Azure Compute Gallery.

Conditions for Azure temporary disk to be eligible for write-back cache disk

You can use the Azure temporary disk as write-back cache disk only if all the following conditions are satisfied:

- The write-back cache disk must non-persist as the Azure temporary disk is not appropriate for persistent data.
- The chosen Azure VM size must include a temporary disk.
- The ephemeral OS disk is not required to be enabled.
- Accept to place the write-back cache file on Azure temporary disk.
- The Azure temporary disk size must be greater than the total size of (write-back cache disk size + reserved space for paging file + 1 GB buffer space).

Non-persistent write-back cache disk scenarios

The following table describes three different scenarios when a temporary disk is used for write-back cache while creating a machine catalog.

SCENARIO	OUTCOME
All conditions to use a temporary disk for write-back cache are satisfied.	The WBC file `mcsdif.vhdx` is placed on the temporary disk.
Temporary disk has insufficient space for write-back cache usage.	A VHD disk 'MCSWCDisk' is created and WBC file `mcsdif.vhdx` is placed on this disk.
Temporary disk has sufficient space for write-back cache usage but `UseTempDiskForWBC` is set to false.	A VHD disk 'MCSWCDisk' is created and WBC file `mcsdif.vhdx` is placed on this disk.

See the following PowerShell topics:

- Create a machine catalog with non-persistent write-back cache disk
- Create a machine catalog with persistent write-back cache disk

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure server-side encryption

Citrix DaaS supports customer-managed encryption keys for Azure managed disks through Azure Key Vault. With this support you can manage your organizational and compliance requirements by encrypting the managed disks of your machine catalog using your own encryption key. For more information, see Server-side encryption of Azure Disk Storage.

When using this feature for managed disks:

- To change the key that the disk is encrypted with, you change the current key in the `DiskEncryptionSet`. All resources associated with that `DiskEncryptionSet` change to be encrypted with the new key.
- When you disable or delete your key, any VMs with disks using that key automatically shut down. After shutting down, the VMs are not usable unless the key is enabled again or you assign a new key. Any catalog using the key cannot be powered on, and you cannot add VMs to it.

Important considerations when using customer-managed encryption keys

Consider the following when using this feature:

- All resources related to your customer-managed keys (Azure Key Vaults, disk encryption sets, VMs, disks, and snapshots) must reside in the same subscription and region.
- Disks, snapshots, and images encrypted with customer-managed keys cannot move to another resource group and subscription.
- Refer to the Microsoft site for limitations on disk encryption sets per region.

NOTE:

See Quickstart: Create a Key Vault using the Azure portal for information on configuring Azure server-side encryption.

Azure Customer-managed encryption key

When creating a machine catalog, you can choose whether to encrypt data on the machines provisioned in the catalog. Server-side encryption with a customer-managed encryption key lets you manage encryption at a managed disk level and protect data on the machines in the catalog. A Disk Encryption Set (DES) represents a customer-managed key. To use this feature, you must first create your DES in Azure. A DES is in the following format:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

Select a DES from the list. The DES you select must be in the same subscription and region as your resources.

If you create a catalog with an encryption key and later disable the corresponding DES in Azure, you can no longer power on the machines in the catalog or add machines to it.

See Create a machine catalog with customer-managed key.

Azure disk encryption at host

You can create an MCS machine catalog with encryption at host capability. Currently, MCS supports only the machine profile workflow for this feature. You can use a VM or a template spec as an input for a machine profile.

This encryption method does not encrypt the data through the Azure storage. The server hosting the VM encrypts the data and then the encrypted data flows through the Azure storage server. Hence, this method of encryption encrypts data end to end.

Restrictions:

Azure disk encryption at the host is:

- Not supported for all Azure machine sizes
- Incompatible with Azure disk encryption

For more information, see:

- Create a machine catalog with encryption at host capability.
- Retrieve encryption at host information from a machine profile

Double encryption on managed disk

You can create a machine catalog with double encryption. Any catalogs created with this feature have all disks server side encrypted with both platform and customer-managed keys. You own and maintain the Azure Key Vault, Encryption Key, and the Disk Encryption Sets (DES).

Double encryption is platform-side encryption (default) and customer-managed encryption (CMEK). Therefore, if you are a high security sensitive customer who is concerned about the risk associated with any encryption algorithm, implementation, or a compromised key, you can opt for this double

© 1997–2026 Citrix Systems, Inc. All rights reserved.

encryption. Persistent OS and data disks, snapshots, and images are all encrypted at rest with double encryption.

NOTE:

- You can create and update a machine catalog with double encryption using Studio and PowerShell commands.
- You can use non-machine profile-based workflow or machine profile-based workflow for creating or updating a machine catalog with double encryption.
- If you use non-machine profile-based workflow to create a machine catalog, you can reuse the stored `DiskEncryptionSetId`.
- If you use a machine profile, you can use a VM or template spec as a machine profile input.

Limitations

- Double encryption is not supported for Ultra Disks or Premium SSD v2 disks.
- Double encryption is not supported on unmanaged disks.
- If you disable a Disk Encryption Set key associated with a catalog, then the VMs of the catalog are disabled.
- All resources related to your customer-managed keys (Azure Key Vaults, disk encryption sets, VMs, disks, and snapshots) must be in the same subscription and region.
- You can only create up to 50 disk encryption sets per region per subscription.

See the following PowerShell topics:

- Create a machine catalog with double encryption
- Convert an unencrypted catalog to use double encryption
- Verify the catalog is double encrypted

Azure resource groups

Azure provisioning resource groups provide a way to provision the VMs that provide applications and desktops to users. You can create a resource group or use an existing resource group to provision VMs in an MCS machine catalog. You can use the same resource group in multiple machine catalogs. For information about Azure resource groups, see the Microsoft documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure Resource Group Usage

There is no limit on the number of virtual machines, managed disks, snapshots, and images per Azure Resource Group. (The limit of 240 VMs per 800 managed disks per Azure Resource Group has been removed.)

- When using a full-scope service principal to create a machine catalog, MCS creates only one Azure Resource Group and uses that group for the catalog.
- When using a narrow scope service principal to create a machine catalog, you must supply an empty, pre-created Azure Resource Group for the catalog.

Azure Marketplace

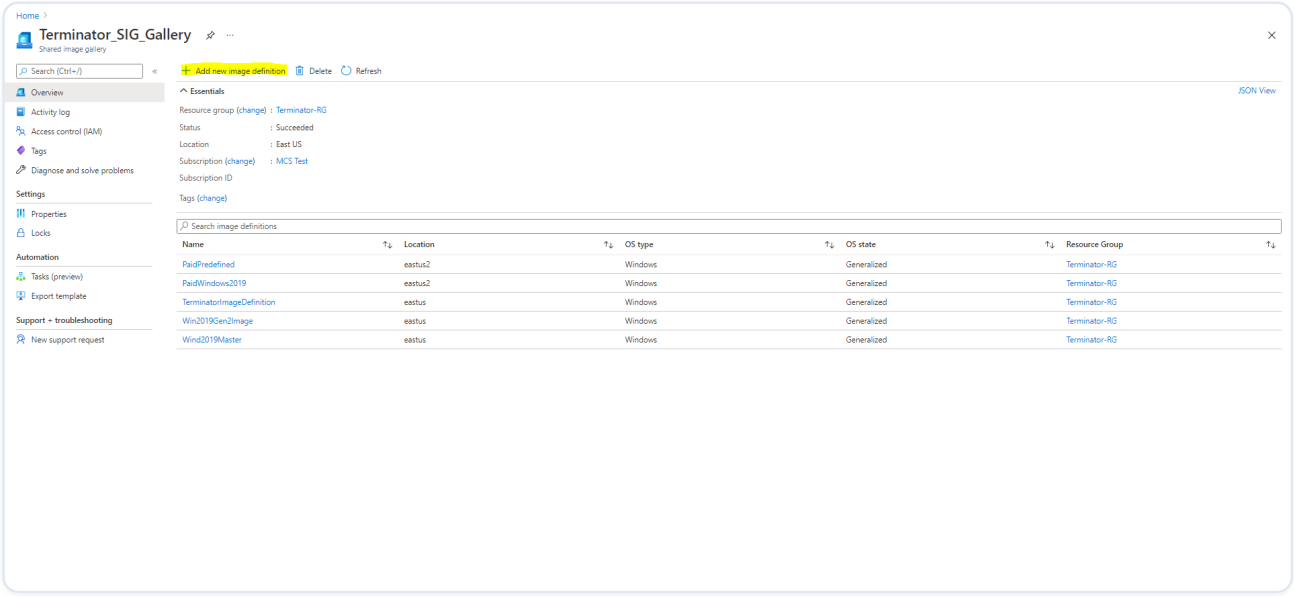
Citrix DaaS supports using a master image on Azure that contains plan information to create a machine catalog. For more information, see Microsoft Azure Marketplace.

TIP:

Some images found on the Azure Marketplace, like the standard Windows Server image, do not append plan information. Citrix DaaS feature is for paid images.

Ensure that the image created in Azure Compute Gallery contains Azure plan information

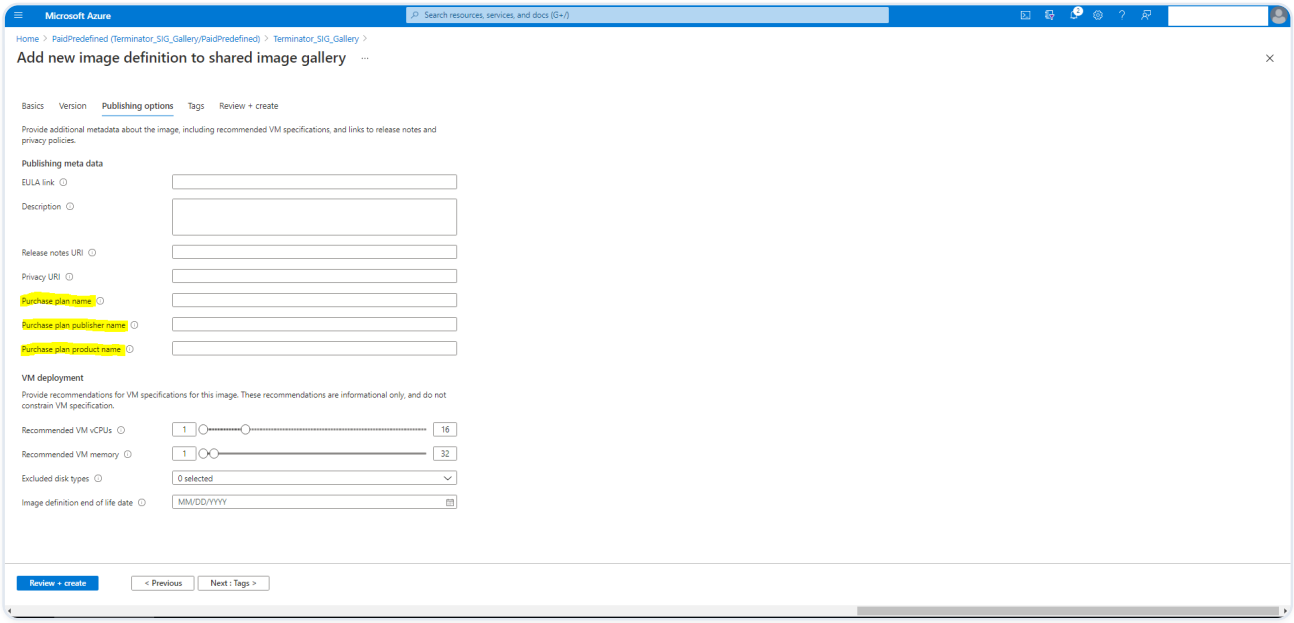
Use the procedure in this section to view Azure Compute Gallery images in Studio. These images can optionally be used for a master image. To put the image into an Azure Compute Gallery, create an image definition in a gallery.



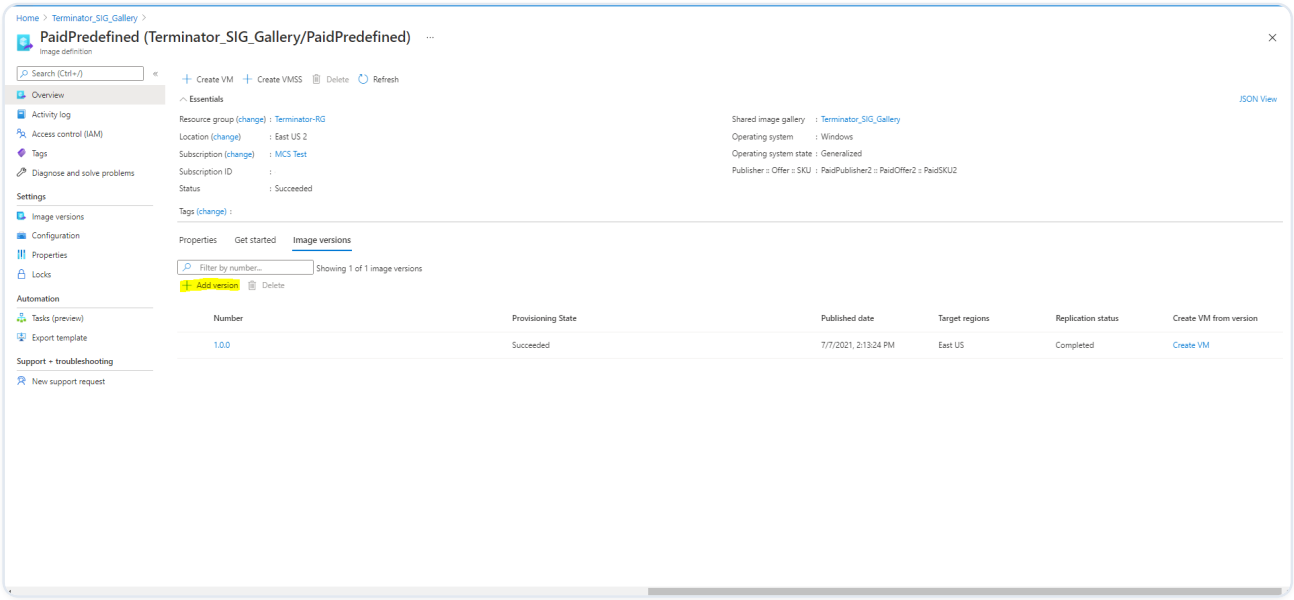
In the **Publishing options** page, verify the purchase plan information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The purchase plan information fields are initially empty. Populate those fields with the purchase plan information used for the image. Failure to populate purchase plan information can cause the machine catalog process to fail.

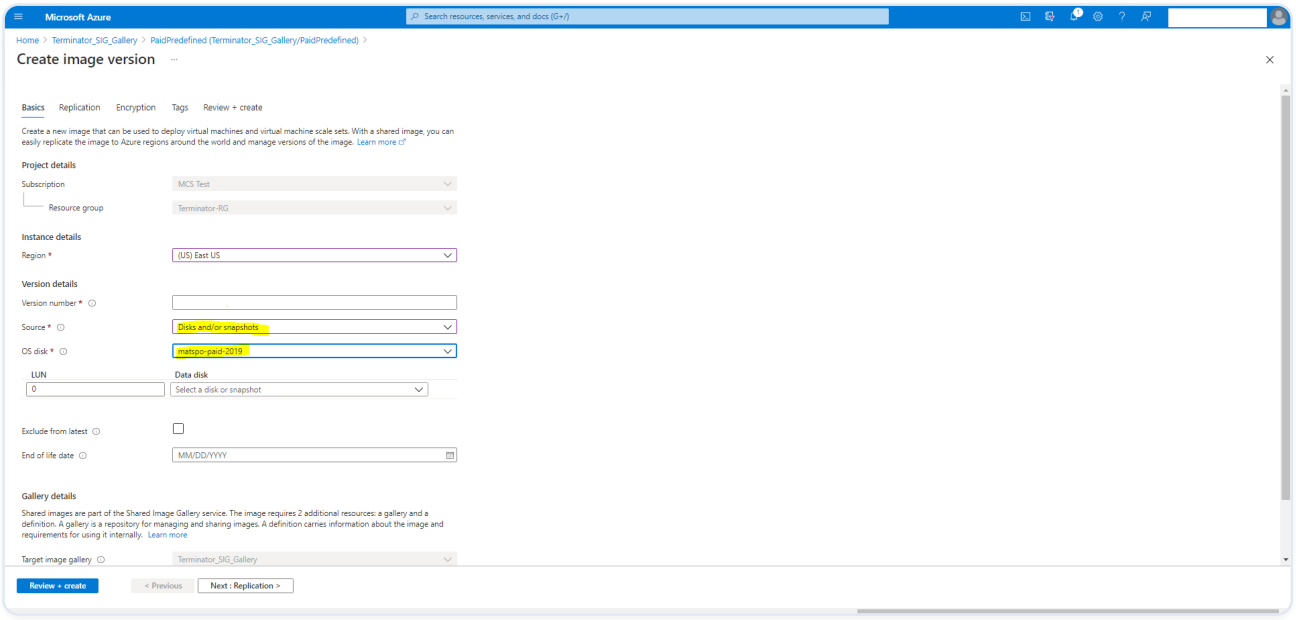


After verifying the purchase plan information, create an image version within the definition. This is used as the master image. Click **Add version**:



In the **Version details** section, select the image snapshot or managed disk as the source:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Provision catalog VMs with Azure Monitor Agent installed

Azure monitoring is a service which you can use to collect, analyze, and act on telemetry data from your Azure and on-premises environments.

Azure Monitor Agent (AMA) collects monitoring data from compute resources like virtual machines and delivers the data to Azure monitor. It currently supports the collection of Event Logs, Syslog, and Performance metrics and sends it to Azure Monitor Metrics and Azure Monitor Logs data sources.

To enable monitoring by uniquely identifying the VMs in monitoring data, you can provision the VMs of an MCS machine catalog with AMA installed as an extension.

Requirements

- Permissions: Ensure that you have the minimum Azure permissions as specified in About Azure permissions and the following permissions to use Azure Monitor:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Data Collection Rule: Set up a data collection rule in the Azure portal. For information about setting up a DCR, see Create a data collection rule. A DCR is platform specific (Windows or Linux). Ensure that you create a DCR as per the required platform. The AMA uses Data

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Collection Rules (DCR) to manage the mapping between the resources, such as VMs, and data sources, like Azure Monitor Metrics and Azure Monitor Logs.

- Default Workspace: Create a workspace in the Azure portal. For information on creating a workspace, see Create a Log Analytics workspace. When you collect logs and data, the information is stored in a workspace. A workspace has a unique workspace ID and resource ID. The workspace name must be unique for a given resource group. After you create a workspace, configure data sources and solutions to store their data in the workspace.
- Whitelisted the monitor extension: The extensions `AzureMonitorWindowsAgent` and `AzureMonitorLinuxAgent` are Citrix defined whitelisted extensions. To view the list of whitelisted extensions, use the PowerShell command, `Get-ProvMetadataConfiguration`.
- Master Image: Microsoft recommends removing extensions from an existing machine before creating a new machine from it. If the extensions are not removed, it might lead to leftover files and unexpected behavior. For more information, see If the VM is recreated from an existing VM.

For information on creating a catalog with AMA enabled using PowerShell, see Provision catalog VMs with AMA enabled.

Azure confidential VMs

Azure confidential computing VMs ensure that your virtual desktop is encrypted in memory and protected in use.

You can use MCS to create a catalog with Azure confidential VMs. You must use the machine profile workflow to create such a catalog. You can use both VM and ARM template spec as a machine profile input.

You can also use a confidential VM type Azure master image and a confidential VM type Azure machine profile to create a prepared image, and then use this prepared image to create an MCS catalog.

Important considerations for confidential VMs

The important considerations for supported VM sizes and creating machine catalog with confidential VMs are as follows:

- To check the VM sizes supported by Confidential VMs, see Sizes.
- Create machine catalogs with confidential VMs.
    - You can create a machine catalog with Azure Confidential VMs using Studio and PowerShell commands.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You must use machine profile-based workflow for creating a machine catalog with Azure Confidential VMs. You can use a VM or template spec as a machine profile input.
- The master image and the machine profile input must be both enabled with the same confidential security type. Different Azure resources use different labels to indicate the confidential VM type.

  For Azure snapshot, managed disk or virtual machine, the security types are:

  - ConfidentialVM_DiskEncryptedWithCustomerKey.
  - ConfidentialVM_DiskEncryptedWithPlatformKey.
  - ConfidentialVM_VMGuestStateOnlyEncryptedWithPlatformKey

  For Azure ARM template spec version, the security types are:

  - VMGuestStateOnly: Confidential VM with only VM guest state encrypted
  - DiskWithVMGuestState: Confidential VM with both OS disk and VM guest state encrypted with platform managed key or customer managed key. Both normal and Ephemeral OS disk can be encrypted.
- You can get confidential VM information of various resource types such as managed disk, snapshot, Azure Compute Gallery image, VM, and ARM template spec using the AdditionalData parameter. For example:

  ```
  PS C:\Users\username> (get-item XDHyp:
  \HostingUnits\mynetwork\image.folder\username-dev-testing-
  rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
  ```

  The additional data fields are:

- DiskSecurityType
- ConfidentialVMDiskEncryptionSetId
- DiskSecurityProfiles

  To get the confidential computing property of a machine size, run the following command: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  The additional data field is `ConfidentialComputingType`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You cannot change the master image or machine profile from confidential to non-confidential security type, or from non-confidential to confidential security type.
- You get appropriate error messages for any incorrect configuration.

Prepare master images and machine profiles

Before creating a set of confidential VMs, follow these steps to prepare a master image and a machine profile for them:

1. In the Azure portal, create a confidential VM with specific settings, such as:
   - **Security Type**: Confidential virtual machines
   - **Confidential OS disk encryption**: Enabled.
   - **Key management**: Confidential disk encryption with a platform-managed key For more information about creating confidential VMs, see this Microsoft article.
2. Prepare the master image on the VM created. Install the necessary applications and VDA on the created VM.

   NOTE:

   Creating confidential VMs using VHD is not supported. Instead, use Azure Compute Gallery, managed disks, or snapshots for this purpose.

3. Create the machine profile using either of these ways:
   - Use the existing VM created in step 1 if it possesses the needed machine properties.
   - If you opt for an ARM template spec as the machine profile, create the template spec as needed. Specifically, configure parameters that meet your confidential VM requirements, such as *SecurityEncryptionType* and *diskEncryptionSet* (for customer-managed key). For more information, see Create an Azure template spec.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Ensure the master image and the machine profile have the same security key type.
- To create confidential VMs requiring confidential OS disk encryption with a customer-managed key, make sure that the disk encryption set IDs in both the master image and the machine profile are identical.

If you want to use a confidential VM type prepared image to create an MCS catalog, then create a prepared image using the confidential VM type master image and a confidential VM type machine profile. See Create an image definition and initial image version for information on creating prepared images.

Create confidential VMs using Studio or PowerShell commands

To create a set of confidential VMs, create a machine catalog using a master image and a machine profile derived from a desired confidential VM.

To create the catalog using Studio, follow the steps described in Create machine catalogs. Keep the following considerations in mind:

- On the **Image** page, select a master image and a machine profile you've prepared for the confidential VM creation. The machine profile selection is mandatory and only profiles that match the same security encryption type as the selected master image are available for selection.
- On the **Virtual Machines** page, only machine sizes that support confidential VMs appear for selection.
- On the **Disk Settings** page, you can't specify the disk encryption set because it's inherited from the selected machine profile.

Boot Integrity Monitoring

If your VM has Secure Boot and virtual Trusted Platform Module (vTPM) enabled, and GuestAttestation extension installed, Microsoft Defender for Cloud can remotely validate that your VM boots in a healthy way. This monitoring is called Boot Integrity Monitoring. For more information on Boot Integrity Monitoring, see Boot integrity monitoring overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can enable Boot Integrity Monitoring for MCS machine catalog VMs (persistent and non-persistent VMs) using a machine profile (VM or template spec). Boot Integrity Monitoring is only supported for Trusted Launch and Confidential VMs.

You can update an existing catalog to use boot integrity using `Set-ProvScheme to point to a boot integrity enabled machine profile. New VMs added to the catalog are then enabled with integrity monitoring.

You can also update an existing VM in a catalog using `Set-ProvVmUpdateTimeWindow`, `Set-ProvVm`, or Maintenance Cycles.

You can convert a:

- VM without integrity monitoring to have integrity monitoring.
- VM with integrity monitoring to without integrity monitoring.

Create machine catalog enabled with integrity monitoring

Ensure that you have the following permissions:

- `Microsoft.Compute/virtualMachines/extensions/read`
- `Microsoft.Compute/virtualMachines/extensions/write`

Do the following to create an MCS machine catalog enabled with integrity monitoring:

1. Create a machine profile (VM or template spec) with `GuestAttestation` extension.
2. Create an MCS machine catalog using the machine profile input using the Full configuration interface or PowerShell commands.

   NOTE:

   You can check the `GuestAttestationExtensionEnabled` status of a VM or template spec using the `Get-Item` PowerShell command with the `AdditionalData parameter`.

3. Add VMs to the catalog.

Create a machine profile enabled with GuestAttestation extension

Create a VM or template spec as a machine profile input with integrity monitoring enabled, which implies `GuestAttestation` extension is installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To create a VM with integrity monitoring enabled, do the following:

1. Sign in to the Azure portal.
2. If you are creating a new VM:
    a. Select **Security type** as **Trusted launch virtual machines** or **Confidential virtual machines**.
    b. Click **Configure security features** and select **Integrity monitoring** checkbox.

    NOTE:

    For integrity monitoring, you must enable Secure Boot and vTPM.

3. On the **Overview** page, go to the **Security type** section and verify that the Security type is Trusted Launch or Confidential virtual machines and Integrity monitoring is enabled.
4. Navigate to the **Extensions + applications** page to verify that `GuestAttestation` is installed.

To enable integrity monitoring of an existing VM, see Enable integrity monitoring-Azure portal.

To create a template spec with `GuestAttestation` extension installed:

1. You can install GuestAttestation using a template spec. See Enable integrity monitoring-template spec.

    NOTE:

    In this template spec, under **Settings**, you can configure the endpoints to use for attestation. If you do not configure, then Azure decides what endpoints to configure.

Create a catalog of on-demand capacity reservation VMs

On-demand capacity reservation enables you to reserve compute capacity in an Azure region or an Availability Zone for any duration of time. For more information on Azure on-demand capacity reservation, see the Microsoft documentation On-demand Capacity Reservation.

You can create an MCS machine catalog of Azure VMs with on-demand capacity reservation using a machine profile (VM or template spec). You can also update an existing machine catalog and existing VMs to have or remove on-demand capacity reservation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature is applicable to persistent and non-persistent machine catalogs.

Limitations

This feature is not applicable to:

- Spot VMs
- Host group
- Hibernation enabled VMs

For more information on limitations, see the Microsoft documentation Limitations and restrictions.

Required permission

You need the following permission for creating a catalog of on-demand capacity reservation VMs:

`Microsoft.Compute/capacityReservationGroups/deploy/action`

Steps to create a catalog of on-demand capacity reservation VMs

1. Create a machine profile source (VM or ARM template spec). For creating a VM or an ARM template spec, see Associate a VM to a Capacity Reservation group.
2. Run the following PowerShell command to check if a machine profile has on-demand capacity reservation enabled or not. If the machine profile is enabled with on-demand capacity reservation, then you get the `capacityReservationGroup id`.

   For example,

   If the machine profile source is a VM, run the following command:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\demand-
   capacity.vm").AdditionalData
   ```

   If the machine profile source is a template spec, run the following command:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
   templatespec.templatespec\14.0.0-capacity-
   reservation.templatespecversion").AdditionalData
   ```

3. Create a machine catalog using a machine profile using Studio or PowerShell commands.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can update a catalog using the `Set-ProvScheme` command. You can also update existing VMs using the PowerShell command `Set-ProvVmUpdateTimeWindow`. The machine profile is updated on the next power on.

Nested virtualization

If you configure the master VM with nested virtualization enabled, then all VMs in the MCS machine catalog created using that master VM has nested virtualization enabled. This feature is applicable to both persistent and non-persistent VMs. You can update an existing MCS machine catalog and existing VMs to have nested virtualization through image update.

Currently, only Dv3 and Ev3 VM sizes support nested virtualization.

For information on nested virtualization, see the Microsoft blog Nested Virtualization in Azure.

NVMe-only SKUs

Typically, the older generations of general purpose, memory optimized, and compute optimized VMs (D/Ev5 or Fv2 and older) support SCSI. The newer generations (Da/Ea/Fav6 and newer) typically support only the NVMe storage interface. MCS supports the NVMe storage controller type to support the new VM SKUs on Azure.

For information on NVMe, see the Microsoft documentation General FAQ for NVMe.

You can create an MCS catalog using a service offering that:

- supports both SCSI and NVMe, see Create a catalog using a service offering that supports both SCSI and NVMe
- supports only NVMe, see Create a catalog using a service offering that supports only NVMe

Limitations

- All service offerings that support NVMe, do not support Trusted Launch at the same time.
- NVMe isn't supported for Gen 1 VMs.
- Some OS images might not support NVMe. In that case, the NVMe option is grayed out on the Azure UI.

Create a catalog using a service offering that supports both SCSI and NVMe

1. Create a VM to be used as a master image.

    a. Use a marketplace image that supports NVMe. A list of Azure Marketplace images that support NVMe can be found at Supported OS images for remote NVMe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Take a snapshot of the OS Disk of the VM to use in the `MasterImageVM` parameter of the `New-ProvScheme` command or use the managed disk directly.

   Check whether your master image supports NVMe or not using one of the following ways:

   - Check the `SupportedDiskControllerTypes` in the `AdditionalData` field of `Get-Item`. For example:

     ```
     (get-item XDHyp:
     \HostingUnits\mynetwork\image.folder\abc.resourcegroup\deg-
     snapshot).AdditionalData
     ```

     The `SupportedDiskControllerTypes` must be `SCSI, NVMe`.

   - Use Azure CLI and PowerShell

2. Use a service offering that supports both NVMe and SCSI.
3. Use a VM or template spec as a machine profile that has NVMe enabled. Take any VM that has `DiskControllerType` set to NVMe. Use the VM directly as a machine profile or export template and use the template spec as a machine profile.

Create a catalog using a service offering that supports only NVMe

1. Create a VM to be used as a master image. Use a marketplace image that supports NVMe. A list of Azure Marketplace images that support NVMe can be found at Supported OS images for remote NVMe.
2. Use a service offering that supports only NVMe.

> **NOTE:**
>
> As the service offering supports NVMe, you do not need a machine profile with `DiskControllerType` set to `NVMe` to enable NVMe on the catalog. However, if you use a machine profile, it must have the `DiskControllerType` either set to `NVMe` or must have it blank or not specified.

Modify existing persistent VMs

NVMe configuration cannot be changed on a VM once it is created. The way to change NVMe configuration for a persistent VM is to redeploy the VM. The logic to do this is:

1. Save the current state of the VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. After powering on an existing VM, detect whether the VM requires redeployment.

    a. If the configuration change is from NVMe to NVMe or SCSI to SCSI, redeployment of the VM is not required.

    b. If the configuration change is from SCSI to NVMe and conversely, redeploy and recreate the VM.

Use PowerShell

This section details how to do the following tasks using PowerShell:

- Use template spec in creating or updating a catalog using PowerShell
- Enable Azure VM extensions
- Machine catalogs with Trusted Launch
- Use machine profile property values
- Configure Availability Zones using PowerShell
- Provision VMs on Azure dedicated hosts
- Configure storage types
- Enable zone-redundant storage
- Capture diagnostic settings on VMs and NICs from a machine profile
- Verify the Windows license
- Configure the Linux license
- Create a machine catalog with an Azure ephemeral disk
- Configure Azure Compute Gallery
- Create or update a catalog with multiple NICs per VM
- Create a machine catalog with non-persistent write-back cache disk
- Create a machine catalog with persistent write-back cache disk
- Improve boot performance with MCSIO
- Create a machine catalog with customer-managed encryption key
- Create a machine catalog with encryption at host capability
- Create a machine catalog with double encryption
- Page file location determination
- Page file setting scenarios

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Specify page file setting
- Modify page file settings
- Provision catalog VMs with AMA enabled
- Create a catalog using Azure Spot VMs
- Configure backup VM sizes
- Copy tags on all resources

Use template spec in creating or updating a catalog using PowerShell

You can create or update an MCS machine catalog using a template spec as a machine profile input. To do this, you can use Studio or PowerShell commands.

For Studio interface, see Create a machine catalog using an Azure Resource Manager image in Studio interface.

Using PowerShell commands:

1. Open the **PowerShell** window.
2. Run `asnp citrix*`.
3. Create or update a catalog.
    - To create a catalog:
        a. Use the `New-ProvScheme` command with a template spec as a machine profile input. For example:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
[<CommonParameters>]
```

b. Finish creating the catalog.

- To update a catalog, use `Set-ProvScheme` command with a template spec as a machine profile input. For example:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'

[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[<CommonParameters>]
```

Enable Azure VM extensions

After you select the ARM template spec, run the following PowerShell commands to work with Azure VM extensions:

- To view the list of supported Azure VM extensions: `Get-ProvMetadataConfiguration`
- To add more VM extensions: `Add-ProvMetadataConfiguration`. For example, `Add-ProvMetadataConfiguration -PluginType "AzureRM" -ConfigurationName "Extension" -ConfigurationValue "CustomScriptExtension"`

  If you try to add any of the following, the command fails with an error message:

  - Citrix defined extension.
  - Existing user defined extension.
  - Unsupported configuration keys. Currently, the supported configuration key is `Extension`.
- To remove extensions from the list: `Remove-ProvMetadataConfiguration`. You can remove the extensions that you added.

Machine catalogs with Trusted Launch

To successfully create a machine catalog with Trusted Launch, use:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A master image enabled with Trusted Launch. You must use a machine profile, however, it is not necessary for the machine profile to be Trusted Launch enabled. If you use a master image enabled with Trusted Launch and a machine profile not enabled with Trusted Launch, you get a warning message because of the mismatched Trusted Launch configuration between master image and machine profile.
- A VM size that supports Trusted Launch.
- A Windows VM version that supports Trusted Launch. Currently, Windows 10, Windows 11, Windows Server 2016, 2019, and 2022 support Trusted Launch.

To view the Citrix DaaS offering inventory items, and to determine whether the VM size supports Trusted Launch, run the following command:

1. Open a PowerShell window.
2. Run **asnp citrix*** to load the Citrix-specific PowerShell modules.
3. Run the following command:

   ```
   $s = (ls XDHyp:\HostingUnits\<name of hosting
   unit>\serviceoffering.folder\"<VM size>".serviceoffering)
   ```

4. Run `$s | select -ExpandProperty Additionaldata`
5. Check the value of the `SupportsTrustedLaunch` attribute.
   - If `SupportsTrustedLaunch` is **True**, the VM size supports Trusted Launch.
   - If `SupportsTrustedLaunch` is **False**, the VM size does not support Trusted Launch.

As per Azure's PowerShell, you can use the following command to determine the VM sizes that support Trusted Launch:

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

The following are examples that describe whether the VM size supports Trusted Launch after you run the Azure PowerShell command.

- *Example 1*: If the Azure VM supports only Generation 1, that VM does not support Trusted Launch. Therefore, the `TrustedLaunchDisabled` capability is not displayed after you run the Azure PowerShell command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- *Example 2*: If the Azure VM supports only Generation 2 and the `TrustedLaunchDisabled` capability is **True**, the Generation 2 VM size is not supported for Trusted Launch.
- *Example 3*: If the Azure VM supports only Generation 2 and the `TrustedLaunchDisabled` capability is not displayed after you run the PowerShell command, the Generation 2 VM size is supported for Trusted Launch.

For more information on Trusted Launch for Azure virtual machines, see the Microsoft document Trusted launch for Azure virtual machines.

Create a machine catalog with Trusted Launch

1. Create a master image enabled with Trusted Launch. See the Microsoft documentation Trusted launch VM Images.
2. Create a VM or template spec with security type as **trusted launch virtual machines**. For more information on creating a VM or template spec, see the Microsoft document Deploy a trusted launch VM.
3. Create a machine catalog using Studio or PowerShell commands.
   - If you want to use Studio, see Create a machine catalog using an Azure Resource Manager image in Studio.
   - If you want to use PowerShell commands, use the `New-ProvScheme` command with the VM or the template spec as a machine profile input.

     Example of `New-ProvScheme` with VM as machine profile input:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

     -MachineProfile "XDHyp:
     \HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
     hine profile vm.vm>"

     -ProvisioningSchemeName <String>

     -HostingUnitName <String>

     -IdentityPoolName <String>
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

Example of `New-ProvScheme` with template spec as machine profile input:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

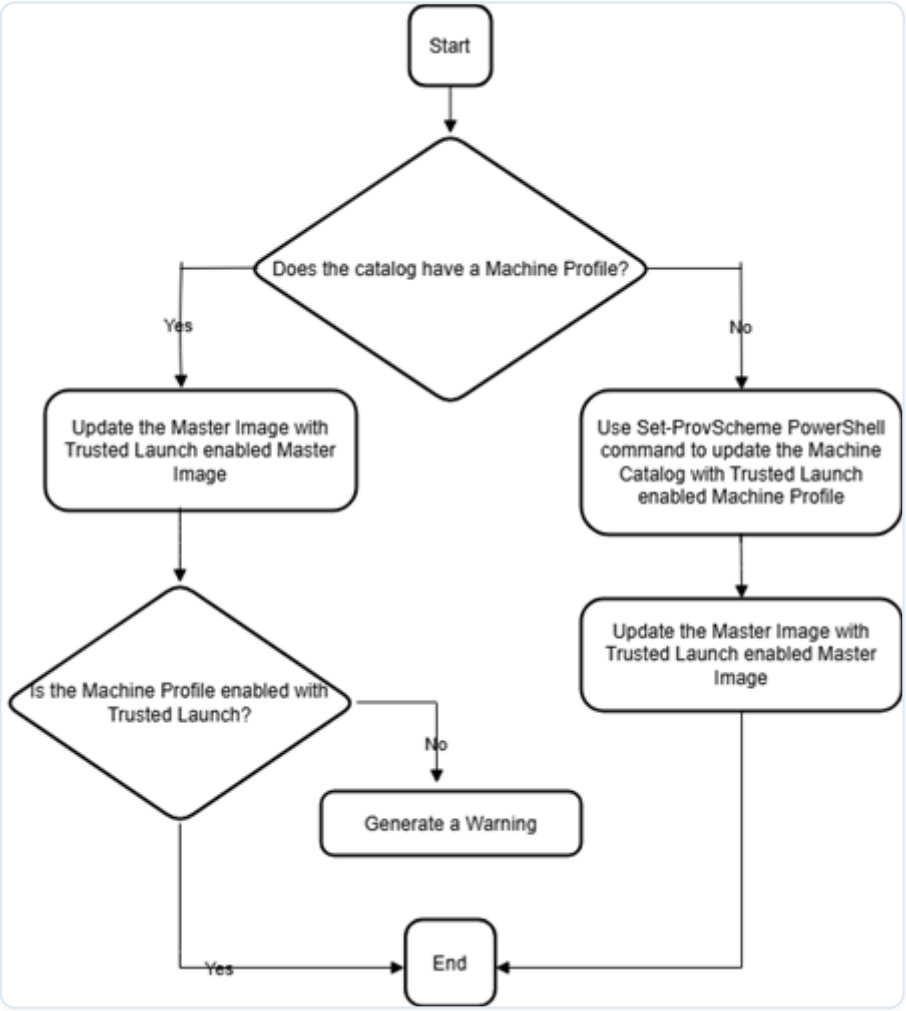
[<CommonParameters>]
```

Update a machine catalog with Trusted Launch

You can update both persistent and non-persistent machine catalogs:

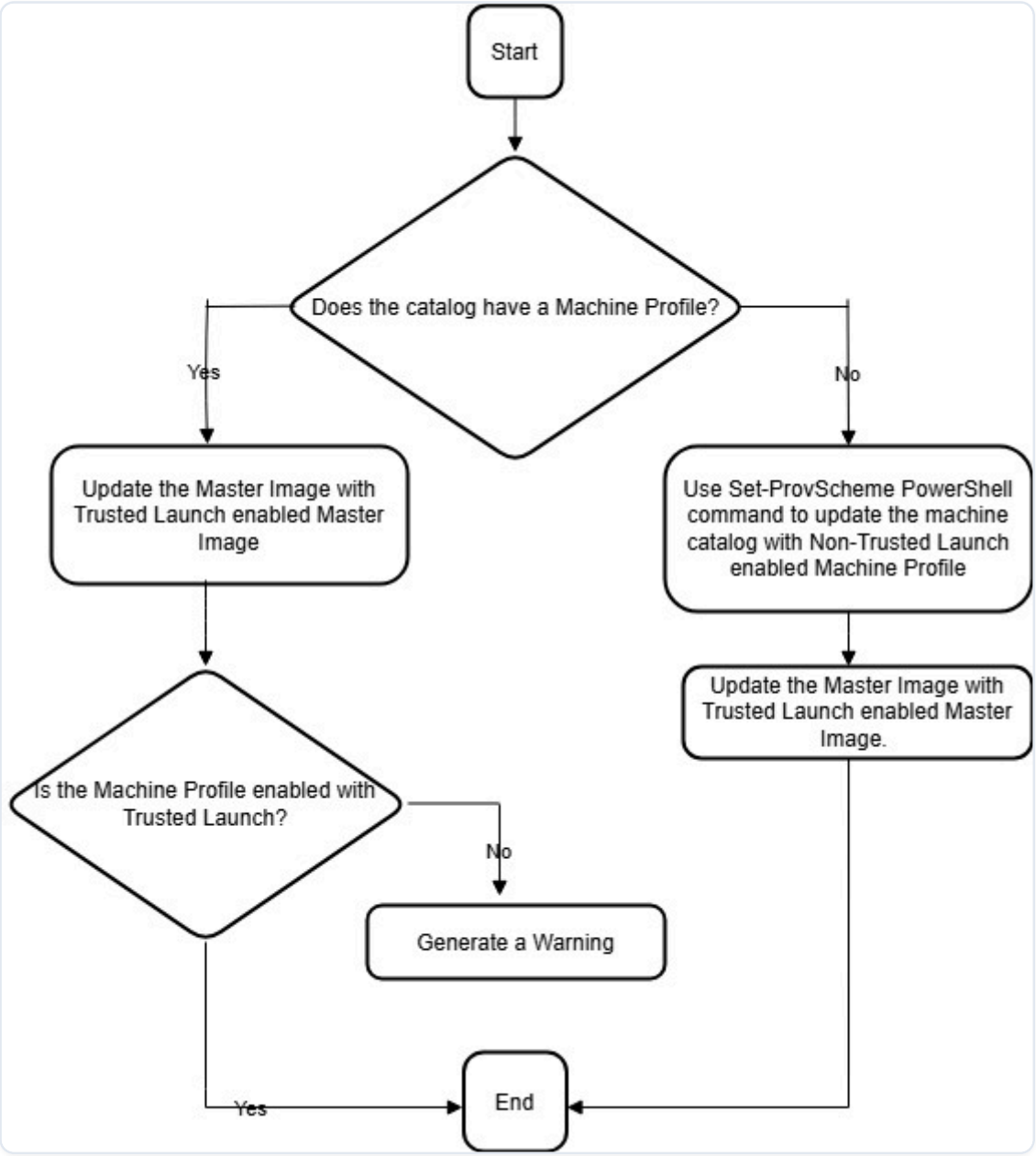
For persistent machine catalog:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For non-persistent machine catalog:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Errors while creating machine catalogs with Trusted Launch

You get appropriate errors in the following scenarios while creating a machine catalog with Trusted Launch:

SCENARIO	ERROR
If you select a machine profile while creating an unmanaged catalog	`MachineProfileNotSupportedForUnmanagedCatalog`
If you select a machine profile that supports Trusted Launch while creating a catalog with unmanaged disk as the master image	`SecurityTypeNotSupportedForUnmanagedDisk`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCENARIO	ERROR
If you select a machine profile with a security type different from the security type of the master image	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
If you select a VM size that does not support Trusted Launch but use a master image that supports Trusted Launch while creating a catalog	`MachineSizeNotSupportTrustedLaunch`

Use machine profile property values

The machine catalog uses the following properties that are defined in the custom properties:

- Availability zone
- Dedicated Host Group Id
- Disk Encryption Set Id
- OS type
- License type
- Storage type

If these custom properties are not defined explicitly, then the property values are set from the ARM template spec or VM, whichever is used as the machine profile. In addition, if `ServiceOffering` is not specified, then it is set from the machine profile.

NOTE:

If some of the properties are missing from the machine profile and not defined in the custom properties, then the default values of the properties take place wherever applicable.

The following section describes some scenarios at `New-ProvScheme` and `Set-ProvScheme` when `CustomProperties` either have all the properties defined or values are derived from the MachineProfile.

- New-ProvScheme Scenarios
  - MachineProfile has all the properties and CustomProperties are not defined. Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfile has some properties and CustomProperties are not defined. Example: MachineProfile only has LicenseType and OsType.

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

</CustomProperties>
```

- Both MachineProfile and CustomProperties define all properties. Example:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

  Custom properties take priority. The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</CustomProperties>
```

- Some properties are defined in MachineProfile and some properties are defined in CustomProperties. Example:
  - CustomProperties define LicenseType and StorageAccountType
  - MachineProfile define LicenseType, OsType, and Zones

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- Some properties are defined in MachineProfile and some properties are defined in CustomProperties. In addition, ServiceOffering is not defined. Example:
  - CustomProperties define StorageType
  - MachineProfile define LicenseType

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- If the OsType is in neither in the CustomProperties nor in the MachineProfile, then:
  - The value is read from the master image.
  - If the master image is an unmanaged disk, the OsType is set to Windows. Example:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

The value from the master image is written to the custom properties, in this case Linux.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Set-ProvScheme Scenarios
  - An existing catalog with:
    - CustomProperties for `StorageAccountType` and OsType
    - MachineProfile `mpA.vm` that defines zones
  - Updates:
    - MachineProfile mpB.vm that defines StorageAccountType
    - A new set of custom properties $CustomPropertiesB that defines LicenseType and OsType

  `Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

  The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- An existing catalog with:
  - CustomProperties for `StorageAccountType` and OsType
  - MachineProfile `mpA.vm` that defines StorageAccountType and LicenseType
- Updates:
  - A new set of custom properties $CustomPropertiesB that defines StorageAccountType and OsType.

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>

</CustomProperties>
```

- An existing catalog with:
  - CustomProperties for `StorageAccountType` and OsType
  - MachineProfile `mpA.vm` that defines Zones
- Updates:
  - A MachineProfile mpB.vm that defines StorageAccountType and LicenseType

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `ServiceOffering` is not specified

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

The following values are set as custom properties for the catalog:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

Configure Availability Zones using PowerShell

Using PowerShell, you can view the Citrix DaaS offering inventory items by using `Get-Item`. For example, to view the *Eastern US region* `Standard_B1ls` service offering:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

To view the zones, use the `AdditionalData` parameter for the item:

`$serviceOffering.AdditionalData`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If Availability Zones are not specified, there is no change in how machines are provisioned.

To configure Availability Zones through PowerShell, use the **Zones** custom property available with the `New-ProvScheme` operation. The **Zones** property defines a list of Availability Zones to provision machines into. Those zones can include one or more Availability Zones. For example, `<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` for Zones 1 and 3.

Use the `Set-ProvScheme` command to update the zones for a provisioning scheme.

If an invalid zone is provided, the provisioning scheme is not updated, and an error message appears providing instructions on how to fix the invalid command.

TIP:

If you specify an invalid custom property, the provisioning scheme is not updated and a relevant error message appears.

Outcome of using host groups and Azure availability zones at the same time

There is a pre-flight check to assess whether the creation of a machine catalog will be successful based on the availability zone specified in the custom property and the host group's zone. Catalog creation fails if the availability zone custom property does not match the host group's zone.

For information on configuring availability zones through PowerShell, see Configuring Availability Zones through PowerShell.

For information on Azure dedicated hosts, see Azure dedicated hosts.

The following table describes the various combinations of availability zone and host group zone and which ones result in successful or failed creation of a machine catalog.

HOST GROUP ZONE	AVAILABILITY ZONE IN CUSTOM PROPERTY	MACHINE CATALOG CREATION OUTCOME
Specified. For example, host group is in Zone 1	Not specified	Successful. Machines are created in the host group's zone
Specified. For example, host group is in Zone 1	Same zone as host group zone. For example, zone in the custom property is set to 1	Successful. Machines are created in Zone 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HOST GROUP ZONE	AVAILABILITY ZONE IN CUSTOM PROPERTY	MACHINE CATALOG CREATION OUTCOME
Specified. For example, host group is in Zone 1	Different from the host group zone. For example, zone in the custom property is set to 2	As the specified availability zone and the host group's zone do not match, catalog creation fails with a relevant error during pre-flight checks
Specified. For example, host group is in Zone 1	Multiple zones specified. For example, zones in the custom properties are set to 1,2 or 2,3	As the specified availability zone and the host group's zone do not match, catalog creation fails with a relevant error during pre-flight checks
Not specified. For example, zone of the host group is `None`	Not specified	As the specified availability zone and the host group's zone match (that is, no zone), catalog creation is successful. Machines are not created in any zone
Not specified. For example, zone of the host group is `None`	Specified. For example, zones in the custom property are set to one or multiple zones	Because the specified availability zone and the host group's zone do not match, catalog creation fails with a relevant error during pre-flight checks

Provision VMs on Azure dedicated hosts

You can use MCS to provision VMs on Azure dedicated hosts. Before provisioning VMs on Azure dedicated hosts:

- Create a host group.
- Create hosts in that host group.
- Ensure that there is sufficient host capacity reserved for creating catalogs and virtual machines.

You can create a catalog of machines with host tenancy defined through the following PowerShell script:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

When using MCS to provision virtual machines on Azure dedicated hosts, consider:

- A *Dedicated host* is a catalog property and cannot be changed once the catalog is created. Dedicated tenancy is currently not supported on Azure.
- A pre-configured Azure host group, in the region of the hosting unit, is required when using the `HostGroupId` parameter.
- Azure auto-placement is required. This functionality makes a request to onboard the subscription associated with the host group. For more information, see VM Scale Set on Azure Dedicated Hosts - Public Preview. If auto-placement is not enabled, MCS throws an error during catalog creation.

Configure storage types

Select different storage types for virtual machines in Azure environments that use MCS. For target VMs, MCS supports:

- OS disk: premium SSD, SSD, or HDD
- Write-back cache disk: premium SSD, SSD, or HDD

When using these storage types, consider the following:

- Ensure that your VM supports the selected storage type.
- If your configuration uses an Azure ephemeral disk, you do not get the option for write-back cache disk setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP:

`StorageType` is configured for an OS type and storage account. `WBCDiskStorageType` is configured for write-back cache storage type. For a normal catalog, `StorageType` is required. If `WBCDiskStorageType` is not configured, the `StorageType` is used as the default for `WBCDiskStorageType`.

If WBCDiskStorageType is not configured, then StorageType is used as the default for WBCDiskStorageType

Configure storage types for VMs

To configure storage types for VMs, use the `StorageType` parameter in `New-ProvScheme`. To update the value of the `StorageType` parameter in an existing catalog to one of the supported storage types use `Set-ProvScheme` command.

The following is an example set of the `CustomProperties` parameter in a provisioning scheme:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

Enable zone-redundant storage

You can select zone-redundant storage during catalog creation. It synchronously replicates your Azure managed disk across multiple availability zones, which allows you to recover from a failure in one zone by utilizing the redundancy in others.

You can specify **Premium_ZRS** and **StandardSSD_ZRS** in the storage type custom properties. ZRS storage can be set using existing custom properties or through the **MachineProfile** template. ZRS storage is also supported with `Set-ProvVMUpdateTimeWindow` command with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`-StartsNow` and `-DurationInMinutes -1` parameters. You can change existing VMs from LRS to ZRS storage.

NOTE:

- `StartsNow` indicates that the scheduled start time is the current time.
- `DurationInMinutes` with a negative number (for example, –1) indicates no upper bound on the schedule's time window.

Limitations:

- Supported only for managed disks
- Supported only with premium and standard solid-state drives (SSD)
- Not supported with `StorageTypeAtShutdown`
- Available only in certain regions.
- Performance of Azure drops when creating ZRS disks at scale. Therefore, for the first power on, turn on the machines in smaller batches (less than 300 machines at a time)

Set zone-redundant storage as the disk storage type

You can select zone-redundant storage during the initial catalog creation, or you can update your storage type in an existing catalog.

Select zone-redundant storage using PowerShell commands

When creating a new catalog in Azure using the `New-ProvScheme` PowerShell command, use `Standard_ZRS` as the value in the `StorageAccountType`. For example:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

When setting this value, it is validated by a dynamic API that determines if it can be used properly. The following exceptions can occur if the use of ZRS is not valid for your catalog:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: The StorageTypeAtShutdown custom property cannot be used with ZRS storage.
- **StorageAccountTypeNotSupportedInRegion**: This exception occurs if you try to use ZRS Storage in an Azure Region that does not support ZRS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ZrsRequiresManagedDisks**: You can use zone-redundant storage only with managed disks.

You can set the disk storage type using the following custom properties:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

NOTE:

During catalog creation, the machine profile's OS disk `StorageType` is used if the custom properties are not set.

Capture diagnostic settings on VMs and NICs from a machine profile

You can capture diagnostic settings on VMs and NICs from a machine profile while creating a machine catalog, updating an existing machine catalog, and updating existing VMs.

You can create a VM or template spec as a machine profile source.

Key steps

1. Set up required IDs in Azure. You must provide these IDs in the template spec.
    - Storage account
    - Log analytics workspace
    - Event hub namespace with the standard tier pricing
2. Create machine profile source.
3. Create a new machine catalog, update an existing catalog, or update existing VMs.

Set up required IDs in Azure

Set up one of the following in Azure:

- Storage account
- Log analytics workspace
- Event hub namespace with the Standard tier pricing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SET UP A STORAGE ACCOUNT

Create a standard storage account in Azure. In the template spec, give the full resourceId for the storage account as the `storageAccountId`.

Once VMs are set up to log data to the storage account, the data can be found under the `insights-metrics-pt1m` container.

SET UP A LOG ANALYTICS WORKSPACE

Create a log analytics workspace. In the template spec, give the full resourceId for the log analytics workspace as the workspaceId.

Once VMs are set up to log data to the workspace, data can be queried under Logs in Azure. You can run the following command in Azure under Logs to show a count of all the metrics logged by a resource:

```
AzureMetrics | summarize Count=count() by ResourceId
```

SET UP AN EVENT HUB

Do the following to set up an event hub in the Azure portal:

1. Create an event hub namespace with the standard tier pricing.
2. Create an event hub underneath the namespace.
3. Navigate to **Capture** under the event hub. Switch ON the toggle to capture with the Avro output type.
4. Create a new container in an existing storage account to capture the logs.
5. In the template spec, specify the `eventHubAuthorizationRuleId` in the following format: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Specify the name of the event hub.

Once VMs are set up to log data to the event hub, the data is captured into the configured storage container.

Create a machine profile source

You can create a VM or template spec as a machine profile source.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CREATE A VM BASED MACHINE PROFILE WITH DIAGNOSTIC SETTINGS

If you want to create a VM as your machine profile, then first set up diagnostic settings on the template VM itself. You can refer to the detailed instructions provided in the Microsoft documentation Diagnostic settings in Azure Monitor.

You can run the following commands to verify that there are now diagnostic settings associated with the VM or NIC:

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

CREATE A TEMPLATE SPEC-BASED MACHINE PROFILE WITH DIAGNOSTIC SETTINGS

If you want to use a VM that already has diagnostic settings enabled and export it into an ARM template spec, these settings won't be automatically included within the template. You must manually add or modify diagnostic settings within the ARM template.

However, if you want a VM as your machine profile, MCS ensures that the critical diagnostic settings are accurately captured and applied to the resources within your MCS catalog.

1. Create a standard template spec that defines a VM and NICs.
2. Add additional resources to deploy the diagnostic settings according to the spec: Microsoft.Insights diagnosticSettings. For scope, reference either a VM or NIC that's in the template by name with a partial ID. For example, for creating diagnostic settings attached to a VM named test-VM in the template spec, specify the scope as:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. Use the template spec as a machine profile source.

Create or update a catalog with diagnostic settings

After you create a machine profile source, you can now create a machine catalog using `New-ProvScheme` command, update an existing machine catalog using `Set-ProvScheme` command, and update existing VMs using `Request-ProvVMUpdate` command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verify the Windows license

You can verify that the provisioned VM is using the licensing benefit by running the following PowerShell command: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- For the Windows Server license type, verify that the license type is **Windows_Server**. More instructions are available at `<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>`.
- For the Windows Client license type, verify that the license type is **Windows_Client**. More instructions are available at `<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>`.

Alternatively, you can use the `Get-Provscheme` PowerShell SDK to do the verification. For example: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. For more information about this cmdlet, see `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>`.

Configure the Linux license

With bring-your-own-subscription (BYOS) Linux licenses, you do not have to pay for the software. The BYOS charge only includes the compute hardware fee. There are two types of licenses:

- **RHEL_BYOS**: To use RHEL_BYOS type successfully, enable Red Hat Cloud Access on your Azure subscription.
- **SLES_BYOS**: The BYOS versions of SLES include support from SUSE.

You can set the LicenseType value to Linux options at `New-ProvScheme` and `Set-ProvScheme`.

Example of setting LicenseType to RHEL_BYOS at `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example of setting LicenseType to SLES_BYOS at `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="SLES_BYOS" /></CustomProperties>'
```

NOTE:

If `LicenseType` value is empty, then the default values are Azure Windows Server License or Azure Linux License, depending on OsType value.

Example of setting LicenseType to empty:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

Create a machine catalog with an Azure ephemeral disk

To provision ephemeral OS disks using `New-ProvScheme`, consider the following constraints:

- The VM size used for the catalog must support ephemeral OS disks.
- The size of the cache or temporary disk associated with the VM size must be greater than or equal to the size of the OS disk.
- The temporary disk size must be greater than the cache disk size.

Also consider these constraints when:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Creating the provisioning scheme
- Modifying the provisioning scheme
- Updating the image

To use ephemeral disks, you must set the custom property `UseEphemeralOsDisk` to **true** when running `New-ProvScheme`.

NOTE:

If the custom property `UseEphemeralOsDisk` is set to **false** or a value is not specified all provisioned VDAs continue to use a provisioned OS disk.

The following is an example set of custom properties to use in the provisioning scheme:

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"

            },

            {

                "Name": "UseSharedImageGallery",

                "Value": "true"

            },

            {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
            },
            {
                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
            },
            {
                "Name": "LicenseType",
                "Value": "Windows_Server"
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

Configure an ephemeral disk for an existing catalog

To configure an Azure ephemeral OS disk for an existing catalog, use the `UseEphemeralOsDisk` parameter in `Set-ProvScheme`. Set the value of the `UseEphemeralOsDisk` parameter to **true**.

NOTE:

To use this feature, you must also enable the parameters `UseManagedDisks` and `UseSharedImageGallery`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

Configure storage type used by ephemeral disks

By default, `Standard_LRS` is the storage type used by the ephemeral OS disk feature. You can set the storage type to use SSDs instead for increased disk IOPS on read operations by specifying the `StorageType` custom property. Current supported values are `Standard_LRS`, `StandardSSD_LRS`, and `Premium_LRS`.

`StorageType` can also be updated on existing ephemeral machines with `Set-ProvScheme` and `Set-ProvVMUpdateTimeWindow`.

Configure Azure Compute Gallery

Use the `New-ProvScheme` command to create a provisioning scheme with Azure Compute Gallery support. Use the `Set-ProvScheme` command to enable or disable this feature for a provisioning scheme and to change the replica ratio and replica maximum values.

Three custom properties were added to provisioning schemes to support the Azure Compute Gallery feature:

`UseSharedImageGallery`

- Defines whether to use the Azure Compute Gallery to store the published images. If set to **True**, the image is stored as an Azure Compute Gallery image, otherwise the image is stored as a snapshot.
- Valid values are **True** and **False**.
- If the property is not defined, the default value is **False**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`SharedImageGalleryReplicaRatio`

- Defines the ratio of machines to gallery image version replicas.
- Valid values are integer numbers greater than 0.
- If the property is not defined, default values are used. The default value for persistent OS disks is 1000 and the default value for non-persistent OS disks is 40.

`SharedImageGalleryReplicaMaximum`

- Defines the maximum number of replicas for each gallery image version.
- Valid values are integer numbers greater than 0 and up to 100. MCS generates an error if you provide a value other than the valid range.
- If the property is not defined, the default value is 10.
- If the property is not defined, the default value is 100.

TIP:

When using Azure Compute Gallery to store a published image for MCS provisioned catalogs, MCS sets the gallery image version replica count based on the number of machines in the catalog, the replica ratio, and the replica maximum. The replica count is calculated by dividing the number of machines in the catalog by the replica ratio (rounding up to the nearest integer value) and then capping the value at the maximum replica count. For example, with a replica ratio of 20 and a maximum of 5, 0–20 machines have one replica created, 21–40 have 2 replicas, 41–60 have 3 replicas, 61–80 have 4 replicas, 81+ have 5 replicas.

Use case: Updating the Azure Compute Gallery replica ratio and replica max

The existing machine catalog uses Azure Compute Gallery. Use the `Set-ProvScheme` command to update the custom properties for all existing machines in the catalog and any future machines:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

Use Case: Converting a snapshot catalog to an Azure Compute Gallery catalog

For this use case:

1. Run `Set-ProvScheme` with the `UseSharedImageGallery` flag set to **True**. Optionally include the `SharedImageGalleryReplicaRatio` and `SharedImageGalleryReplicaMaximum` properties.
2. Update the catalog.
3. Power cycle the machines to force an update.

For example:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

TIP:

The parameters `SharedImageGalleryReplicaRatio` and `SharedImageGalleryReplicaMaximum` are not required. After the `Set-ProvScheme` command completes the Azure Compute Gallery image has not yet been created. Once the catalog is configured to use the gallery, the next catalog update operation stores the published image in the gallery. The catalog update command creates the gallery, the gallery image, and the image version. Power cycling the machines updates them, at which point the replica count is updated, if appropriate. From that time, all existing non-persistent machines are reset using the Azure Compute Gallery image and all newly provisioned machines are created using the image. The old snapshot is cleaned up automatically within a few hours.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use Case: Converting an Azure Compute Gallery catalog to a snapshot catalog

For this use case:

1. Run `Set-ProvScheme` with the `UseSharedImageGallery` flag set to **False** or not defined.
2. Update the catalog.
3. Power cycle the machines to force an update.

For example:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

TIP:

Unlike updating from a snapshot to an Azure Compute Gallery catalog, the custom data for each machine is not yet updated to reflect the new custom properties. Run the following command to see the original Azure Compute Gallery custom properties: `Get-ProvVm -ProvisioningSchemeName catalog-name`. After the `Set-ProvScheme` command completes the image snapshot has not yet been created. Once the catalog is configured to not use the gallery, the next catalog update operation stores the published image as a snapshot. From that time, all existing non-persistent machines are reset using the snapshot and all newly provisioned machines are created from the snapshot. Power cycling the machines updates them, at which point the custom machine data is updated to reflect that `UseSharedImageGallery` is set to **False**. The old Azure Compute Gallery assets (gallery, image, and version) are automatically cleaned up within a few hours.

Create or update a catalog with multiple NICs per VM

MCS supports multiple NICs per VM. You can associate multiple NICs on a VM to multiple subnets, however, those subnets must be in the same virtual network (VNet). You can use PowerShell command to:

- Create a catalog with multiple NICs on a VM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Update an existing catalog configuration to have multiple NICs on a VM so that newly created VMs have multiple NICs
- Update an existing VM to have multiple NICs

You can create or update a non-machine profile-based machine catalog and machine profile-based machine catalog to have multiple NICs on a VM. Currently, for a machine profile-based machine catalog, you can only have the same number of NICs as specified in the machine profile source.

Property such as accelerated networking is derived from the machine profile source.

NOTE:

The VM size must support the same number of NICs and corresponding accelerated networking, otherwise you get an error.

You can retrieve the maximum number of NICs associated with a selected VM size. A PowerShell property called `MaxNetworkInterfaces` displays the maximum NIC count when you run the PowerShell `get-item` command with the `AdditionalData` parameter.

Retrieve the maximum NIC count

To retrieve the maximum NIC count:

1. Open a **PowerShell** window from the Delivery Controller™ host.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` to list all available VM sizes.
4. Run `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`
5. Check `MaxNetworkInterfaces` to know the maximum NIC count.

Create a catalog with multiple NICs on a VM

To create a catalog with multiple NICs on a VM, do the following:

1. Open a PowerShell window from the Delivery Controller host.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create an identity pool if not already created.
4. Create the provisioning scheme:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If creating a non-machine profile-based machine catalog, run `New-ProvScheme` command with `NetworkMappings` parameter. You can add multiple subnets to the parameter `NetworkMappings`. For example:

```
New-Provscheme -NetworkMappings
@{"0"="subnetpath1";"1"="subnetpath1"}
```

- If creating a machine profile-based machine catalog:

  a. Create a VM in Azure to have multiple NICs. For information, see Create and manage a Windows virtual machine that has multiple NICs. You can also create a new VM, and then attach a network interface in the Networking page of Azure portal.

  b. Run `New-ProvScheme` command with the VM as a machine profile input.

NOTE:

When creating a machine profile-based machine catalog, the count of `NetworkMappings` must be the same as the `NetworkInterfaceCount` of the machine profile. The `NetworkInterfaceCount` can be retrieved from `AdditionalData` of `Get-item -Path "machine profile path"`.

5. Finish creating the catalog.

Update a catalog to have multiple NICs on a VM

To update a catalog to have multiple NICs on a VM, do the following:

1. Open a **PowerShell** window from the Delivery Controller host.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Update the provisioning scheme:

   - If creating a non-machine profile-based machine catalog, run the `Set-ProvScheme` command with `NetworkMappings` parameter. You can add multiple subnets to parameter `NetworkMappings`. For example:

```
Set-Provscheme -NetworkMappings
@{"0"="subnetpath1";"1"="subnetpath1"}
```

   - If creating a machine catalog based on a machine profile:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Create a VM in Azure to have multiple NICs. For information, see Create and manage a Windows virtual machine that has multiple NICs.

b. Run `Set-ProvScheme` command with the VM as a machine profile input.

Update an existing VM to have multiple NICs on a VM

You can also update an existing VM using `Set-ProvVMUpdateTimeWindow` and also perform power cycle on existing VM during the update time window. For more information on updating an existing VM, see Update provisioned machines to current provisioning scheme state.

Create a machine catalog with non-persistent write-back cache disk

To configure a catalog with non-persistent write-back cache disk, use the PowerShell parameter `New-ProvScheme CustomProperties`. The custom properties are:

- `UseTempDiskForWBC`. This property indicates whether you are accepting to use the Azure temporary storage to store the write-back cache file. This must be configured to true when running `New-ProvScheme` if you want to use the temporary disk as write-back cache disk. If this property is not specified, the parameter is set to False by default.

For example, using the `CustomProperties` parameter to set `UseTempDiskForWBC` to true:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</CustomProperties>'
```

NOTE:

After you commit the machine catalog to use Azure local temporary storage for write-back cache file, it cannot be changed to use VHD later.

Create a machine catalog with persistent write-back cache disk

To configure a catalog with persistent write-back cache disk, use the PowerShell parameter `New-ProvScheme CustomProperties`.

TIP:

Use the PowerShell parameter `New-ProvScheme CustomProperties` only for cloud-based hosting connections. If you want to provision machines using a persistent write-back cache disk for an on-premises solution (for example, XenServer®) PowerShell is not needed because the disk persists automatically.

This parameter supports an extra property, `PersistWBC`, used to determine how the write-back cache disk persists for MCS provisioned machines. The `PersistWBC` property is only used when the `UseWriteBackCache` parameter is specified, and when the `WriteBackCacheDiskSize` parameter is set to indicate that a disk is created.

NOTE:

This behavior applies to both Azure and GCP where the default MCSIO write-back cache disk is deleted and re-created when power cycling. You can choose to persist the disk to avoid the deletion and recreation of MCSIO write-back cache disk.

Examples of properties found in the `CustomProperties` parameter before supporting `PersistWBC` include:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

NOTE:

This example only applies to Azure. The properties are different in the GCP environment.

When using these properties, consider that they contain default values if the properties are omitted from the `CustomProperties` parameter. The `PersistWBC` property has two possible values: **true** or **false**.

Setting the `PersistWBC` property to **true** does not delete the write-back cache disk when the Citrix DaaS administrator shuts down the machine from the management interface.

Setting the `PersistWBC` property to **false** deletes the write-back cache disk when the Citrix DaaS administrator shuts down the machine from the management interface.

NOTE:

If the `PersistWBC` property is omitted, the property defaults to **false** and the write-back cache is deleted when the machine is shut down from the management interface.

For example, using the `CustomProperties` parameter to set `PersistWBC` to true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

IMPORTANT:

The `PersistWBC` property can only be set using the `New-ProvScheme` PowerShell cmdlet. Attempting to alter the `CustomProperties` of a provisioning scheme after creation has no impact on the machine catalog and the persistence of the write-back cache disk when a machine is shut down.

For example, set `New-ProvScheme` to use the write-back cache while setting the `PersistWBC` property to true:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`" /
>

</CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Improve boot performance with MCSIO

You can improve boot performance for Azure and GCP managed disks when MCSIO is enabled. Use the PowerShell `PersistOSDisk` custom property in the `New-ProvScheme` command to configure this feature. Options associated with `New-ProvScheme` include:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To enable this feature, set the `PersistOSDisk` custom property to **true**. For example:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Create a machine catalog with customer-managed encryption key

If you want to create a machine catalog using PowerShell commands, where the encryption key is a customer-managed key, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Enter `cd xdhyp:/`.
4. Enter `cd .\HostingUnits\(your hosting unit)`.
5. Enter cd diskencryptionset.folder.
6. Enter dir to get the list of the Disk Encryption Sets.
7. Copy the Id of a Disk Encryption Set.
8. Create a custom property string to include the Id of the Disk Encryption Set. For example:

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. Create an identity pool if not already created. For example:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. Run the New-ProvScheme command: For example:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. Finish creating the machine catalog.

Create a machine catalog with encryption at host capability

To create a machine catalog with encryption at host capability

1. Check if the subscription has the encryption at host feature enabled or not. To do this, see `<https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/>`. If not enabled, you must enable the feature for the subscription. For information on enabling the feature for your subscription, see `<https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`.
2. Check if a particular Azure VM size supports encryption at host or not. To do this, in a PowerShell window, run one of the following:

```
PS XDHyp:\Connections\<your connection>\east
us.region\serviceoffering.folder>
```

```
PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Create a VM or a template spec, as an input for machine profile, in the Azure portal with encryption at host enabled.

   - If you want to create a VM, select a VM size that supports encryption at host. After you create the VM, the VM property **Encryption at host** is enabled.
   - If you want to use a template spec, assign the parameter `Encryption at Host` as **true** inside `securityProfile`.

4. Create an MCS machine catalog with machine profile workflow by either selecting a VM or a template spec.

   - OS disk / Data Disk: Gets encrypted through Customer-managed key and Platform-managed key
   - Ephemeral OS Disk: Gets encrypted only through Platform-managed key
   - Cache Disk: Gets encrypted through Customer-managed key and Platform-managed key

   You can create the machine catalog using Studio or running PowerShell commands.

Retrieve encryption at host information from a machine profile

You can retrieve the encryption at host information from a machine profile when you run the PowerShell command with the `AdditionalData` parameter. If `EncryptionAtHost` parameter is **True**, it indicates that the encryption at host is enabled for the machine profile.

For example: When the machine profile input is a VM, run the following command:

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

For example: When the machine profile input is a template spec, run the following command:

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

Create a machine catalog with double encryption

You can create and update a machine catalog with double encryption using Studio and PowerShell commands.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The detailed steps on how to create a machine catalog with double encryption are:

1. Create an Azure Key Vault and DES with Platform-managed and customer-managed keys. For information on how to create an Azure Key Vault and a DES, see Use the Azure portal to enable double encryption at rest for managed disks.
2. To browse available Disk Encryption Sets in your hosting connection:

   a. Open a **PowerShell** window.

   b. Run the following PowerShell commands:

      i. `asnp citrix*`

      ii. `cd xdhyp:`

      iii. `cd HostingUnits`

      iv. `cd YourHostingUnitName (ex. azure-east)`

      v. `cd diskencryptionset.folder`

      vi. `dir`

   You can use an Id of the `DiskEncryptionSet` to create or update a catalog using custom properties.
3. If you want to use machine profile workflow, create a VM or template spec as a machine profile input.

   - If you want to use a VM as a machine profile input:

     a. Create a VM in Azure Portal.

     b. Navigate to **Disks>Key management** to encrypt the VM directly with any `DiskEncryptionSetID`.

   - If you want to use a template spec as a machine profile input:

     a. In the template, under `properties>storageProfile>osDisk>managedDisk`, add `diskEncryptionSet` parameter and add the id of the double encryption DES.
4. Create the machine catalog.

   - If using Studio, do one of the following in addition to the steps in Create machine catalogs.

     - If you do not use a machine-profile based workflow, on the **Disk Settings** page, select **Use the following key to encrypt data on each machine**. Then, select your double encryption DES from the drop-down list. Continue creating the catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If using the machine profile workflow, on the **Image** page, select a master image (or prepared image) and a machine profile. Make sure that the machine profile has a disk encryption set id in its properties.

All machines created in the catalog are double encrypted by the key associated with the DES that you selected.

- If using PowerShell commands, do one of the following:
  - If not using machine profile-based workflow, add the custom property `DiskEncryptionSetId` in the `New-ProvScheme` command. For example:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If using machine profile-based workflow, use a machine profile input in the `New-ProvScheme` command. For example:

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1

-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

Finish creating a catalog using the remote PowerShell SDK. All machines created in the catalog are double encrypted by the key associated with the DES you selected.

Convert an unencrypted catalog to use double encryption

You can update a machine catalog's encryption type (using custom properties or machine profile).

- If not using machine profile-based workflow, add the custom property DiskEncryptionSetId in the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- If using machine profile-based workflow, use a machine profile input in the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

Once successful, all new VMs that you add in your catalog are double encrypted by the key associated with the DES you selected.

Verify the catalog is double encrypted

- In Studio:
  a. Navigate to **Machine Catalogs**.
  b. Select the catalog that you want to verify. Click the **Template Properties** tab located near the bottom of the screen.
  c. Under **Azure Details**, verify the Disk Encryption Set ID in **Disk Encryption Set**. If the catalog's DES Id is blank, the catalog is not encrypted.
  d. In the Azure Portal, verify that the encryption type of the DES associated with the DES Id is platform-managed and customer-managed keys.
- Using the PowerShell command:
  a. Open the **PowerShell** window.
  b. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
  c. Use `Get-ProvScheme` to get the information of your machine catalog. For example:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

  d. Retrieve the DES Id custom property of the machine catalog. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. In the Azure Portal, verify that the encryption type of the DES associated with the DES Id is platform-managed and customer-managed keys.

Page file location determination

The page file location is determined according to the following scenario:

NOTE:

The default page file location is OS disk.

SCENARIO	LOCATION
Page file setting is specified in the custom properties	As specified in the custom properties
Ephemeral OS disk or hibernation is enabled	OS disk
VM has a temporary disk	Temporary disk
MCS IO is enabled	WBC disk

Page file setting scenarios

The following table describes some of the possible scenarios of page file setting during image preparation and provisioning scheme update:

DURING	SCENARIO	OUTCOME
Image preparation	You set the source image page file on the temporary disk, while the VM size that you specify in the provisioning scheme has no temporary disk	The page file is placed on the OS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DURING	SCENARIO	OUTCOME
Image preparation	You set the source image page file on the OS disk, while the VM size that you specify in the provisioning scheme has a temporary disk	The page file is placed on the temporary disk
Image preparation	You set the source image page file on the temporary disk and enable the ephemeral OS disk in the provisioning scheme	The page file is placed on the OS disk
Provisioning scheme update	You attempt to update the provisioning scheme when the VDA version is earlier than 2311	Modifies the page file setting with a warning
Provisioning scheme update	You attempt to update the provisioning scheme when the VDA version is 2311 or later	Determines the page file location as per Page file location determination

Specify page file setting

Using PowerShell commands, you can specify page file settings, including the location and size. This overrides the page file settings determined by MCS as per Page file location determination. You can do this by running the following `New-ProvScheme` command during machine catalog creation.

Important considerations

Consider the following before proceeding with the catalog creation:

- You must provide all the custom properties ('PageFileDiskDriveLetterOverride', 'InitialPageFileSizeInMB', and 'MaxPageFileSizeInMB') in the `New-ProvScheme` command or none of them.
- This feature is not supported through Citrix Studio.
- The initial page file size must be between 16 MB and 16777216 MB.
- The maximum page file size must be greater than or equal to the initial page file size and less than 16777216 MB.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can set both the initial page file size and maximum page file size to zero at the same time.

NOTE:

You can modify the page file settings of the newly added VMs of an existing catalog, without updating the master image. To modify the page file settings, you need VDA version 2311 or later. You can modify the page file settings using the PowerShell commands. For more information, see Modify page file settings.

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "zijinnet" `

-IdentityPoolName "PageFileSettingExample" `

-ProvisioningSchemeName "PageFileSettingExample" `

-InitialBatchSizeHint 1 `

-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-
resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3ef
eea88f.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\zijinnet\
\virtualprivatecloud.folder\\East US.region\\virtualprivatecloud.folder\
\neal-zijincloud-resources.resourcegroup\\neal-zijincloud-resources-
vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.folder\
\Standard_B2ms.serviceoffering" `

-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="d"/> `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

</CustomProperties>'
```

Modify page file settings

You can modify the page file settings of the newly added VMs to an existing catalog without updating the master image. Currently, this feature is applicable to only Azure environments.

To modify the page file settings, you need VDA version 2311 or later. You can modify the page file settings using the PowerShell commands.

Following are the various page file settings that you can modify in the Azure environment:

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

Modify the page file settings of an existing catalog

To modify the page file settings of an existing machine catalog, run the `Set-ProvScheme` command. In this case, the updates are applied only to the new VMs added to the catalog. For example:

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="StorageType"
Value="StandardSSD_LRS" />

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="D" />

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048" />

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property  xsi:type="StringProperty" Name="Zones" Value="1" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
test-group1" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

NOTE:

If you enable the write-back cache and try to set the `PageFileDiskDriveLetterOverride` to `C:` using the PowerShell command, MCS I/O driver automatically redirects the page file to a correct disk drive and not `C:`.

Provision catalog VMs with AMA enabled

1. Set up a machine profile template.
    - If you want to use a VM as a machine profile template:
        a. Create a VM on the Azure portal.
        b. Power on the VM.
        c. Add the VM to the data collection rule under **Resources**. This invokes agent installation on the template VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you must create a Linux catalog, set up a Linux machine.

- If you want to use template spec as a machine profile template:

  a. Set up a template spec.

  b. Add the following extension and data collection rule association to the generated template spec:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",

"apiVersion": "2022-03-01",

"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],

"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,

    "enableAutomaticUpgrade": true

}

},
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you have a data collection rule setup with a Microsoft Sentinel data connector, you can simply add `dataCollectionRuleAssociation` in the template spec in the same manner as a regular DCR association. The catalog VMs can then show up in the Sentinel DCR and the AMA would be installed on those VMs. For information on the best practices for data collection rule creation, see Best practices for data collection rule creation and management in Azure Monitor.

2. Create or update an existing MCS machine catalog.

   - To create a new MCS catalog:

     a. Select that VM or template spec as a machine profile in Studio.

     b. Proceed with the next steps to create the catalog.

   - To update an existing MCS catalog, use the following PowerShell commands. In this case, only the new VMs get the updated machine profile template.

     ```
     Set-ProvScheme -ProvisioningSchemeName "name"

     -MachineProfile "XDHyp:
     \HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
     machine-profile.vm"
     ```

   - To update existing VMs with the updated machine profile template, run `Set-ProvScheme`, and then run `Set-ProvVMUpdateTimeWindow`:

     ```
     Set-ProvScheme -ProvisioningSchemeName "name" -MachineProfile
     "XDHyp:
     \HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
     machine-profile.vm"

     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

3. Power on catalog VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Go to the Azure portal and check if the monitor extension is installed on the VM and the VM is showing up under DCR's Resources. After a few minutes monitoring data is displayed on the Azure Monitor.

Troubleshooting

For information in troubleshooting guidance for Azure Monitor Agent, see the following:

- `<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/>`
- `<https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/>`

Create a catalog using Azure Spot VMs

Azure Spot VMs allow you to take advantage of Azure's unused computing capacity at a significant cost savings. However, the ability to allocate an Azure Spot VM depends on the current capacity and pricing. Therefore, Azure might evict your running VM, fail to create the VM, or fail to power on the VM as per the Eviction policy. Therefore, Azure Spot VMs are good for some non-critical applications and desktops. For more information, see Use Azure Spot Virtual Machines.

Limitations

- All VM sizes aren't supported for Azure Spot VMs. For more information, see Limitations.

  You can run the following PowerShell command to check whether a VM size supports Spot VMs or not. If a VM size supports Spot VM, then `SupportsSpotVM` is **True**.

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").AdditionalData
  ```

- Currently, Azure Spot VMs do not support hibernation.

Requirement

While creating the machine profile source (VM or template spec) for Azure Spot VMs catalog, you must select Azure Spot Instance (if using VM) or set `priority` as `Spot` (if using template spec).

Steps to create a catalog using Azure Spot VMs

1. Create a machine profile source (VM or launch template).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For creating a VM using the Azure portal, see Deploy Azure Spot Virtual Machines using the Azure portal.
- For creating a template spec, add the following properties under **resources > type: Microsoft.Compute/virtualMachines > properties** in the template spec. For example:

```
"priority": "Spot",

"evictionPolicy": "Deallocate",

"billingProfile": {

"maxPrice": 0.01

}
```

NOTE:

- Eviction policy can be **Deallocate** or **Delete**.
- For non-persistent VMs, MCS always sets the eviction policy as **Delete**. If the VM is evicted, it is deleted along with any non-persistent disks (For example, OS disk). Any persistent disks (for example, Identity disk) are not deleted. However, an OS disk is persistent if the catalog type is persistent or the `PersistOsDisk` custom property is set to True. Similarly, a WBC disk is persistent if the `PersistWbc` custom property is set to **True**.
- For persistent VMs, MCS always sets the eviction policy as Deallocate. If the VM is evicted, it is deallocated. No changes are made to the disks.
- The maximum price is the price that you are willing to pay per hour. If you are using **Capacity Only**, then this is **-1**. The maximum price can only be null, -1, or a decimal greater than zero. For more information, see Pricing.

2. You can run the following PowerShell command to check if a machine profile is Azure Spot VM enabled or not. If the `SpotEnabled` parameter is **True** and `SpotEvictionPolicy` is set to **Deallocate** or **Delete**, then the machine profile is Azure Spot VM enabled. For example,

   - If the machine profile source is a VM, run the following command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
delete.vm"). AdditionalData
```

- If the machine profile source is a template spec, run the following command:

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
templatespec.templatespec\14.0.0-spot-
delete.templatespecversion").AdditionalData
```

3. Create a machine catalog using a machine profile with `New-ProvScheme` PowerShell command.

You can update a catalog using the `Set-ProvScheme` command. You can also update existing VMs using the PowerShell command `Set-ProvVmUpdateTimeWindow`. The machine profile is updated on the next power on.

Evictions on a running Azure Spot VM

If the computing capacity is unavailable or the price per hour is higher than the maximum price as configured, Azure evicts a running Spot VM. By default, you are not notified of an eviction. The VM simply freezes and the VM is evicted. Microsoft recommends using Scheduled Events to monitor evictions. See Continuously monitor for eviction. You can also run scripts from within a VM to get a notification before the eviction. For example, Microsoft has a polling script in Python ScheduledEvents.cs.

Troubleshooting

- You can see Spot VM properties in the provisioned VM's customMachineData using the `Get-ProvVM` command. If the priority field is set to **Spot**, then Spot is in use.
- You can check if a VM is using Spot in Azure Portal:

  a. Find the VM in the Azure Portal.

  b. Go to the **Overview** page.

  c. Scroll down to the bottom and locate the **Azure Spot** section.

    - If Spot is not in use, then this field is empty.
    - If Spot is in use, the **Azure Spot** and **Azure Spot eviction policy** fields are set.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. You can check the billing profile or maximum price per hour for the VM on the Configuration page.

Configure backup VM sizes

Public clouds can run out of capacity for a specific VM size. When Azure lacks capacity, MCS falls back to a preconfigured list of backup VM sizes. This curated list, tailored by the customer to their workload requirements, increases the likelihood that one of these sizes has sufficient capacity to boot on Power On or Resume if the VM was previously hibernated.

When a power action is initiated, MCS implements an automated fallback sequence to ensure high availability. The workflow is as follows:

1. Initiation: A user or administrator issues a **PowerOn** or **Resume** command via Web Studio.
2. Exception Monitoring: MCS attempts to start the VM using the primary configuration. It monitors for specific Azure capacity exceptions likeQuota Exceeded, Allocation Failed orZonal Allocation Failed and SKU Not Available(Can just go general on this and say we monitor Azure for any capacity or allocation failures)
3. Sequential Fallback: If one of the above errors occurs, MCS automatically iterates through the BackupVmConfiguration list sequentially until the VM successfully starts. If all sizes in the BackupVmConfiguration fail, the power action is marked as failed.
4. Update vs. Re-creation Logic:
    - Direct Update: In most cases, MCS performs a simple VM size update to the backup SKU and then powers the VM on.
    - Delete and Re-create: To maintain environment integrity, certain transitions require the existing VM to be deleted and a new one created in its place. This occurs when:
        - Switching between Spot and Regular VM types.
        - Switching between VM sizes with Resource Disk (Temporary Storage) support and those without.
5. Data Persistence & Recovery: During a "Delete and Re-create" operation, if all backup sizes also fail due to extreme Azure capacity shortages, the VM may temporarily disappear from the Azure Portal. However, no data loss occurs. Upon the next PowerOn attempt, MCS will recreate the VM using the original settings and reattach the existing OS, Identity, and Data disks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Spot VM Billing & MaxPrice Behavior If your primary configuration utilizes a Machine Profile (VM Template) with Spot priority and a specific Billing Profile (MaxPrice), the following logic applies during fallback:
    - Primary Size: Uses the MaxPrice defined in your Machine Profile. Eviction is based on Price or Capacity.
    - Backup Spot Sizes: The BackupVmConfiguration property does not currently support a unique `MaxPrice` input for each SKU, MCS handles the transition as follows:
    - MaxPrice Reset: MCS sets the MaxPrice to -1.
    - Eviction Policy Shift: This changes the Azure eviction behavior from Price-based to Capacity-based.
    - Pricing: You will be charged the current Spot price, capped at the standard Pay-As-You-Go (PAYG) rate for that backup SKU. This ensures the VM is only evicted if Azure truly runs out of physical capacity, rather than because of a price fluctuation.
7. Persistence of Backup State: Once started, the VM remains on the backup size for the duration of the session until a Shutdown or Hibernate request is processed.
8. Restoration of Primary Size: Upon the next PowerOn or Resume, MCS always attempts to "home" the VM back to its Primary Service Offering (as defined in the Catalog or Machine Profile). If the primary size remains unavailable, the fallback sequence repeats.

Challenges with hibernation

Azure does not allow size changes on a hibernated VM, as explained General limitations. The VM must be in a Stopped state. Therefore, before changing the size, MCS issues a Deallocate request to clear the hibernated state, which causes the VM's hibernation state to be lost. MCS then loops over the backup sizes, updates the VM size, and powers it on.

Backup VM size unsupported scenarios

The following configurations are unsupported:

- For persistent VMs, the following scenarios are unsupported:
    - VM uses DiskControllerType SCSI, but Backup VM size supports only DiskControllerType NVMe.
    - VM uses DiskControllerType NVMe, but Backup VM size supports only DiskControllerType SCSI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For non-persistent VMs with MCSIO enabled, switching to a size without temporary storage is unsupported if the write-back cache disk uses Resource Disk temporary storage.

Prerequisites to configure Backup VM sizes

If any of the following are unmet, an error is thrown.

- Supported only when the Machine Profile is in use on the Machine Catalog.
- Type is optional and can be either Spot or Regular. Defaults to Regular if unspecified.
- Each combination of ServiceOffering must be unique to avoid repeated configurations.
- Regional Quota must have enough cores for the ServiceOffering.
- Network interface count must not exceed the maximum allowed for a ServiceOffering.
- ServiceOfferings in this BackupVmConfiguration list must be compatible with current Custom Properties, capabilities of the Master Image and the MachineProfile. Some failure scenarios are:
  - Azure Dedicated Hosts: Hosts in the Host Group must support the ServiceOffering if dedicated hosts are used.
  - Ephemeral OS Disk: ServiceOffering must support Ephemeral OS Disks if enabled in custom properties.
  - Premium Storage: ServiceOffering must support Premium storage if specified in custom properties.
  - Accelerated Networking: ServiceOffering must support Accelerated Networking if it is enabled in MachineProfile.
  - DiskEncryptionAtHost: ServiceOffering must support Encryption at Host if enabled in MachineProfile.
  - Temporary Storage: If MCSIO is in use and Write Back Cache is on the Temporary disk, use of a VM size that does not have Temporary Storage is not allowed.
  - HyperVGeneration: ServiceOffering must be compatible with the VM generation (1 or 2) specified in MasterImageVM.
  - TrustedLaunch: ServiceOffering must support TrustedLaunch if enabled in MachineProfile.
  - Confidential VMs: ServiceOffering must support Confidential VM if enabled in MachineProfile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a catalog with backup VM sizes

NOTE:

To address the issue of the Studio UI freezing, replace all the single quotes with `"` while running the PowerShell commands.

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create a Broker catalog. This catalog is populated with machines which are about to be created.
4. Create an identity pool. This becomes a container for AD accounts created for the machines that are to be created.
5. Create a provisioning scheme with the machine profile. See How to configure backup configuration.
6. Update the `BrokerCatalog` with the unique Id of the provisioning scheme.
7. Create and add VMs to the catalog.

Update an existing catalog

You can update a provisioning scheme using the `Set-ProvScheme` command. See How to configure backup configuration.

Update existing VMs

You can update existing VMs in a catalog using `Set-ProvVMUpdateTimeWindow` PowerShell command. The command updates the VMs created from the provisioning scheme associated with the catalog on the next power on within the given time window. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
```

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

You can configure the backup VM size list for a selected number of existing MCS VMs using the `Set-ProvVM` command. However, to apply the updates, set an update time window for the VMs using `Set-ProvVMUpdateTimeWindow` and start the VMs within the window. For example,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Run the `Set-ProvVM` command to configure the backup VM size list for a selected existing MCS VM. For example:

```
Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
Name=`"BackupVmConfiguration`" Value=`"[{&quot;ServiceOffering&quot;:
&quot;Standard_D2as_v4&quot;, &quot;Type&quot;: &quot;Spot&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Regular&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Spot&quot;}]`"/>
</CustomProperties>"
```

2. Run the `Set-ProvVMUpdateTimeWindow` command to apply the updates. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

Copy tags on all resources

You can copy tags specified in a machine profile to all the resources such as, multiple NICs and disks (OS disk, Identity disk, and write-back cache disk) of a new VM or an existing VM in a machine catalog. The machine profile source can be a VM or an ARM template spec.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You must add the policy on the tags (See Assign policy definitions for tag compliance) or add the tags in a machine profile source to retain the tags on the resources.

Prerequisites

Create the machine profile source (VM or ARM template spec) to have tags on VM, disks, and NICs of that VM.

- If you want to have a VM as a machine profile input, then apply tags on the VM and all the resources in the Azure portal. See Apply tags with Azure portal.
- If you want to have ARM template spec as a machine profile input, then add the following tag block under each resource.

```
 "tags": {

"TagC": "Value3"

},
```

NOTE:

You can have a maximum of one disk and at least one NIC in the template spec.

Copy tags to the resources of a VM in a new machine catalog

1. Create a non-persistent or persistent catalog with a VM or ARM template spec as a machine profile input.
2. Add a VM to the catalog and power it on. You must see the tags specified in the machine profile copied to the corresponding resources of that VM.

NOTE:

You get an error if there is a mismatch in the number of NICs provided in the machine profile and the number of NICs you want the VMs to use.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Modify tags on the resources of an existing VM

1. Create a machine profile with the tags on all the resources.
2. Update the existing machine catalog with the updated machine profile. For example:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. Turn off the VM on which you want to apply the updates.
4. Request a scheduled update for the VM. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. Turn on the VM.
6. You must see the tags specified in the machine profile copied to the corresponding resources.

NOTE:

You get an error if there is a mismatch in the number of NICs provided in the machine profile and the number of NICs provided in the `Set-ProvScheme`.

Create a preformatted WBC disk catalog

You can create a preformatted WBC disk catalog to improve startup performance of provisioned machines. To implement this functionality, create an Azure catalog with WBC enabled and include an additional custom property `PreformatWriteBackCache` as `True`.

You can update an existing catalog using the `Set-ProvScheme` command to update the WBC disk size.

This feature is compatible with the Image management workflow where MCS separates the mastering phase from the overall provisioning workflow. For information on Image management, see Image management.

Example of creating an Azure catalog with WBC enabled and `PreformatWriteBackCache` as `True`:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

Example of updating the WBC disk cache size of an existing catalog:

```
Set-ProvScheme -ProvisioningSchemeName provisioningschemename
-WriteBackCacheDiskSize 127
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Delete WBC disk at shutdown for MCS provisioned Citrix Provisioning™ catalogs

While creating an MCS provisioned Citrix Provisioning catalogs in Azure, you can provision the WBC disk to be non-persistent (`PersistWBC` as False). This configuration helps to delete the write-back cache (WBC) disk after you shut down the VM for MCS provisioned Citrix Provisioning catalogs in Azure.

Condition:

You must set the custom property `PreformatWriteBackCache` as `True` for this feature to work.

Example of creating an Azure catalog with `PersistWBC` as `False` and `PreformatWriteBackCache` as `True`:

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

You can also update an existing catalog using the `Set-ProvScheme` command to update the `PersistWBC` custom property.

Provision data disk

You can create and assign a persistent data disk to an MCS created persistent or non-persistent VM of an MCS machine catalog in Azure.

The data disk must be provisioned from a managed disk as an image source.

Data disk properties

The data disk derives properties from custom properties or OS disk template if the properties are not specified in the custom properties.

- Properties derived from custom properties
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`
- Properties derived from OS disk template if not specified in custom properties
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`

NOTE:

- If Zone Redundant Storage (ZRS) is not specified in custom properties or OS disk template, then the data disk is placed in the same zone as the OS disk and Identity disk.
- Tags are derived only from the OS disk template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations

The following operations are currently not supported:

- Provisioning of more than one data disk.
- Provisioning of non-persistent data disks.
- Creating a data disk with a template.
- Modifying existing catalogs and VMs to use data disks.
- Resetting the data disk.
- Image update of the data disk.
- Using a source other than a managed disk.
- Storing data disk in Azure Compute Gallery (ACG).
- Using `StorageTypeAtShutdown` for the data disk

Create a catalog with data disk

Include the following parameters in the `New-ProvScheme` PowerShell command to provision an MCS machine catalog with data disk.

- `DataDisk`: Path to a valid ManagedDisk type of inventory item.
- `DataDiskPersistence`: To indicate whether the `DataDisk` is persistent or non-persistent. However, currently, only persistent data disks are supported.

For example:

```
New-ProvScheme  -CleanOnBoot -HostingUnitName "<HostingUnitName >"
-IdentityPoolName "<IdentityPoolName >" -InitialBatchSizeHint 1
-MasterImageVM disk.manageddisk -NetworkMapping <NetworkMapping >
-ProvisioningSchemeName "<ProvisioningSchemeName >" -DataDisk "XDHyp:
\HostingUnits\Azure-Resources-1\image.folder\<resourcegroupname>\xxxx-
datadisk.manageddisk"  -DataDiskPersistence "Persistent"  -Scope @()
-VMCpuCount 4  -VMMemoryMB 6144  -TenancyType Shared  -FunctionalLevel
"L7_20"
```

Determine if a data disk is in use

Do the following to verify if the data disk is assigned to a VM:

- Run `Get-ProvVm` and check the VM's `CustomVmData`. If the VM is using the data disk, there is a disk record with role `DiskRole.DataDisk`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Check if a data disk is present under the VM in the Azure portal.

Delete a data disk

If you delete the catalog, the data disk is deleted unless you use `forgetVM` or `purgeDBOnly` option. If you delete the VM, the data disk is deleted unless you use the `forgetVM` or `purgeDBOnly` option.

Migrate from unmanaged to managed disks

On September 30, 2025, Azure will officially retire unmanaged disks (that is, VHDs). Any existing VMs using unmanaged disks will be stopped and deallocated after the deadline.

However, you can migrate your MCS provisioned VMs from unmanaged to managed disks, which helps to avoid service outages due to Azure's unmanaged disk retirement plans.

All unmanaged disks attached to the VM are converted. This includes the Identity Disk, OS Disk, and WBC Disk (if used).

For more information on Azure's unmanaged disk retirement plan, see Migrate your Azure unmanaged disks by September 30, 2025.

Use cases

This feature applies to persistent and non-persistent MCS-provisioned catalogs.

It also supports migration for both on-demand and non-on-demand (legacy) VMs:

- On-Demand VMs: Transition your existing disks from unmanaged to managed disks to align with Azure's updated support.
- Non-On-Demand (Legacy) VMs: Legacy or non-on-demand VMs only support unmanaged disks. Use this feature to convert your legacy VMs to on-demand while also migrating to managed disks.

For more information on on-demand provisioning, see Azure on-demand provisioning.

Limitations

- Once a machine catalog or VM is converted to managed disks, it cannot be converted back to unmanaged disks
- For non-on-demand (legacy) VMs, the migration process includes converting them to on-demand provisioning. You cannot convert the disks only and continue to use non-on-demand VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Important considerations

- Conversion does not occur automatically. It happens as part of a power-on operation.
- If multiple updates are requested for a VM, the disk conversion takes precedence. Additional updates are deferred until a subsequent power on.
- Once the VM is successfully converted and powered on, VHDs for the VM are cleaned up to save costs. The storage account itself are not cleaned up.
  - A base disk might still exist in the storage account. You can run a catalog update, and a new snapshot (or ACG) basedisk is created.
  - Once all the VMs in the catalog are converted and the new basedisk is created, the empty storage account can be deleted.

Required permissions

You need the following permission on your Azure Service Principal to allow conversion from unmanaged to managed disks:

```
Microsoft.Compute/virtualMachines/convertToManagedDisks/write
```

Configuration steps

For On-Demand Catalogs:

1. Run `Set-ProvScheme` (or `Set-ProvVM` for persistent VMs)to update `UseManagedDisks` to `True`. For example:

```
Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"UseManagedDisks`" Value=`"true`" /></CustomProperties>"
```

```
Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
name>" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /
></CustomProperties>"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Run `Set-ProvVMUpdateTimeWindo`w` to apply the updates. In this example, the update is applied on the next power on for the VM.

```
Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
-VMName "<vm-name>"
```

3. Power on the VMs.

For Non-On-Demand (Legacy) Catalogs:

1. Run `Set-ProvScheme` (or `Set-ProvVM` for persistent VMs) to configure `Set DeploymentSchema` to `1.1`. For example:

```
Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"DeploymentSchema`" Value=`"1.1`" /></CustomProperties>"
```

```
Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
name>" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"DeploymentSchema`" Value=`"1.1`" /
></CustomProperties>
```

2. Run `Set-ProvVMUpdateTimeWindow` to apply the updates. In this example, the update is applied on the next power on for the VM.

```
Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
-VMName "<vm-name>"
```

3. Power on the VMs.

Troubleshooting

If a VM fails to convert from unmanaged to managed disks:

- Verify that the `UseManagedDisks` or `DeploymentSchema` custom properties are set correctly:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - If using `Set-ProvScheme`, verify the ProvScheme custom properties by running `Get-ProvScheme`. For more information, see Get-ProvScheme.
  - If using `Set-ProvVM`, verify the VM has a new configuration with the updated custom property by running `Get-ProvVMConfiguration`. For more information, see Set-ProvVM.

- Verify that the following permission is present in your Azure Service Principal:
  - `Microsoft.Compute/virtualMachines/convertToManagedDisks/write`
- Run `Get-ProvOperationEvent` to view any warnings for the Provisioning Scheme. For more information, see Get-ProvOperationEvent. For example:

```
Get-ProvOperationEvent -LinkedObjectType ProvisioningScheme
-LinkedObjectUid <your-provscheme-id>
```

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a Microsoft Azure catalog.

More information

- Create and manage connections and resources
- Connection to Microsoft Azure Resource Manager
- Create machine catalogs

Create a Microsoft SCVMM catalog

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Microsoft System Center Virtual Machine Manager (VMM) virtualization environments.

NOTE:

Before creating a VMM catalog, you need to finish creating a connection to VMM. See Connection to Microsoft System Center Virtual Machine Manager.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a master VM

- Install a VDA on the master VM, and select the option to optimize the desktop. This improves performance.
- Take a snapshot of the master VM to use as a backup.
- Create virtual desktops.

MCS on SMB 3 file shares

For machine catalogs created with MCS on SMB 3 file shares for VM storage, credentials must meet the following requirements to ensure that calls from the XenServer® Communications Library (HCL) connect successfully to SMB storage.

- VMM user credentials must include full read write access to the SMB storage.
- Storage-virtual disk operations during VM lifecycle events are performed through the Hyper-V server using the VMM user credentials.

For more information on SMB 3, see Overview of file sharing using the SMB 3 protocol in Windows Server.

When using VMM 2012 SP1 with Hyper-V on Windows Server 2012: When using SMB as storage, enable the Authentication Credential Security Support Provider (CredSSP) from the Cloud Connector to individual Hyper-V machines. For more information, see CTX137465.

Using a standard PowerShell V3 remote session, the HCL in the Cloud Connector uses CredSSP to open a connection to the Hyper-V machine. This feature passes Kerberos-encrypted user credentials to the Hyper-V machine, and the PowerShell commands in the session on the remote Hyper-V machine run with the credentials provided (in this case, those of the VMM user), so that communication commands to storage work correctly.

The following tasks use PowerShell scripts that originate in the HCL. The scripts are then sent to the Hyper-V machine to act on the SMB 3.0 storage.

Consolidate Master Image: An image creates a new MCS provisioning scheme (machine catalog). It clones and flattens the master VM ready for creating new VMs from the new disk created (and removes dependency on the original master VM).

ConvertVirtualHardDisk on the root\\virtualization\\v2 namespace

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

Create differencing disk: Creates a differencing disk from the image generated by consolidating the image. The differencing disk is then attached to a new VM.

CreateVirtualHardDisk on the root\\virtualization\\v2 namespace

Example:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

Upload identity disks: The HCL cannot directly upload the identity disk to SMB storage. Therefore, the Hyper-V machine must upload and copy the identity disk to the storage. Because the Hyper-V machine cannot read the disk from the Cloud Connector, the HCL must first copy the identity disk through the Hyper-V machine as follows.

1. The HCL uploads the Identity to the Hyper-V machine through the administrator share.
2. The Hyper-V machine copies the disk to the SMB storage through a PowerShell script running in the PowerShell remote session.

   A folder is created on the Hyper-V machine and the permissions on that folder are locked for the VMM user only (through the remote PowerShell connection).
3. The HCL deletes the file from the administrator share.
4. When the HCL completes the identity disk upload to the Hyper-V machine, the remote PowerShell session copies the identity disks to SMB storage, and then deletes it from the Hyper-V machine.

The identity disk folder is recreated if deleted to make it available for reuse.

Download identity disks: As with uploads, the identity disks pass through the Hyper-V machine to the HCL. The following process creates a folder that has only VMM user permissions on the Hyper-V server if it does not exist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. The HyperV machine copies the disk from the SMB storage to local Hyper-V storage using a PowerShell script running in the PowerShell V3 remote session.
2. HCL reads the disk from the Hyper-V machine's administrator share into memory.
3. HCL deletes the file from the administrator share.

Create catalog with a machine profile

You can use a machine profile to create and update an MCS machine catalog in System Center Virtual Machine Manager (SCVMM) environments. You can enable vTPM. You can also add custom tags of a machine profile VM to the provisioned VMs.

Important considerations

- Master image can only be a snapshot and not a VM.
- You can only use VM as the machine profile source.
- In System Center Virtual Machine Manager (SCVMM) environments, you can use a machine profile to create and update an MCS machine catalog. You can enable vTPM and/or Secure Boot. You can also add custom tags from a machine profile VM to provisioned VMs.
- If the master image has vTPM enabled, then you must enable the vTPM on the machine profile source.
- vTPM is only supported on Generation 2 machines.
- The following parameters overwrite the values captured in a machine profile if provided separately:
  - VMCpuCount
  - VMMemoryMB
  - Disk storage
- The custom tags are inherited only from the machine profile and not from the master image. The `CitrixProvisioningSchemeId` tag is added by default to the VM. If you do not want to include the `CitrixProvisioningSchemeId` tag, then add the `-NoVmTagging` parameter while creating a hosting unit. Example:

```
New-Item -HypervisorConnectionName  $ConnectionName `

-NetworkPath @($NetworkPath) `

-Path @($HostingUnitPath) `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-PersonalvDiskStoragePath @() `
-RootPath $RootPath `
-StoragePath @($StoragePath) `
-NoVmTagging
```

- You can update an existing catalog using the `Set-ProvScheme` command.

SUPPORT MATRIX

MASTER IMAGE	MACHINE PROFILE	RESULT
No vTPM	vTPM	Cloned machines get vTPM enabled
vTPM	vTPM	Cloned machines get vTPM enabled
vTPM	No vTPM	Preflight error - operation blocked
No vTPM	No vTPM	Cloned machines have no vTPM

Create a machine catalog using a machine profile

1. Create a VM to be a machine profile source. For more information, see Provision virtual machines in the VMM fabric. You cannot change the **Generation** once selected. You can do the following in SCVMM:
    - To enable vTPM:
        a. After you create the VM, log in to the Hyper-V host and find your VM under the **Hyper-V Manager**.
        b. Right-click the VM, then go to **Settings**.
        c. Under **Security**, select the **Enable Trusted Platform Module** checkbox.
2. Open a **PowerShell** window.
3. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Create a Broker catalog. This catalog is populated with machines which are about to be created.
5. Create an identity pool. This becomes a container for AD accounts created for the machines that are to be created.
6. Create a provisioning scheme with the machine profile. For example:

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. Updates the Broker catalog with the unique Id of the provisioning scheme.
8. Create and add VMs to the catalog.

Update an existing catalog

You can update an existing catalog using the Set-ProvScheme command. For example:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

Remove a VM

You can choose to remove a VM from a catalog but not delete the VM from the SCVMM. In this case, the `CitrixProvisioningSchemeId` tag is only removed from the VM. The custom tags are not deleted from the VM. You can remove a VM using Studio or PowerShell commands.

REMOVE A VM USING STUDIO

1. Select and right-click the VM.
2. Click **Delete**.
3. Select **Remove the virtual machines from the catalog but do not delete the virtual machines**.

USING POWERSHELL COMMANDS

`Remove-ProvVM` with `ForgetVM` parameter. For more information, see:

- Remove tags

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Delete machines without hypervisor access

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a Microsoft System Center Virtual Machine Manager catalog.

More information

- Create and manage connections and resources
- Connection to Microsoft System Center Virtual Machine Manager
- Create machine catalogs

Create a Nutanix catalog

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Nutanix virtualization environments.

NOTE:

Before creating a Nutanix catalog, you need to finish creating a connection to Nutanix. See Connection to Nutanix.

Create a machine catalog using Nutanix machine template version

When creating an MCS-provisioned machine catalog with a Citrix-managed Nutanix AHV Prism Central host connection, the base image is created from a Nutanix VM template version. A key advantage is that Nutanix Prism Central allows a VM template to be used across multiple clusters. As a result, Citrix administrators can use a single Nutanix VM template version as the master VM for multiple MCS machine catalogs, even if those catalogs are on different Nutanix clusters.

Before creating the catalog, create a master VM, and convert it to a VM template version in Nutanix Prism Central. See Nutanix documentation for the steps.

You can create a catalog using:

- Studio. You can also create a catalog using existing VMs. See Create a machine catalog using existing machines (power managed)
- PowerShell commands

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations

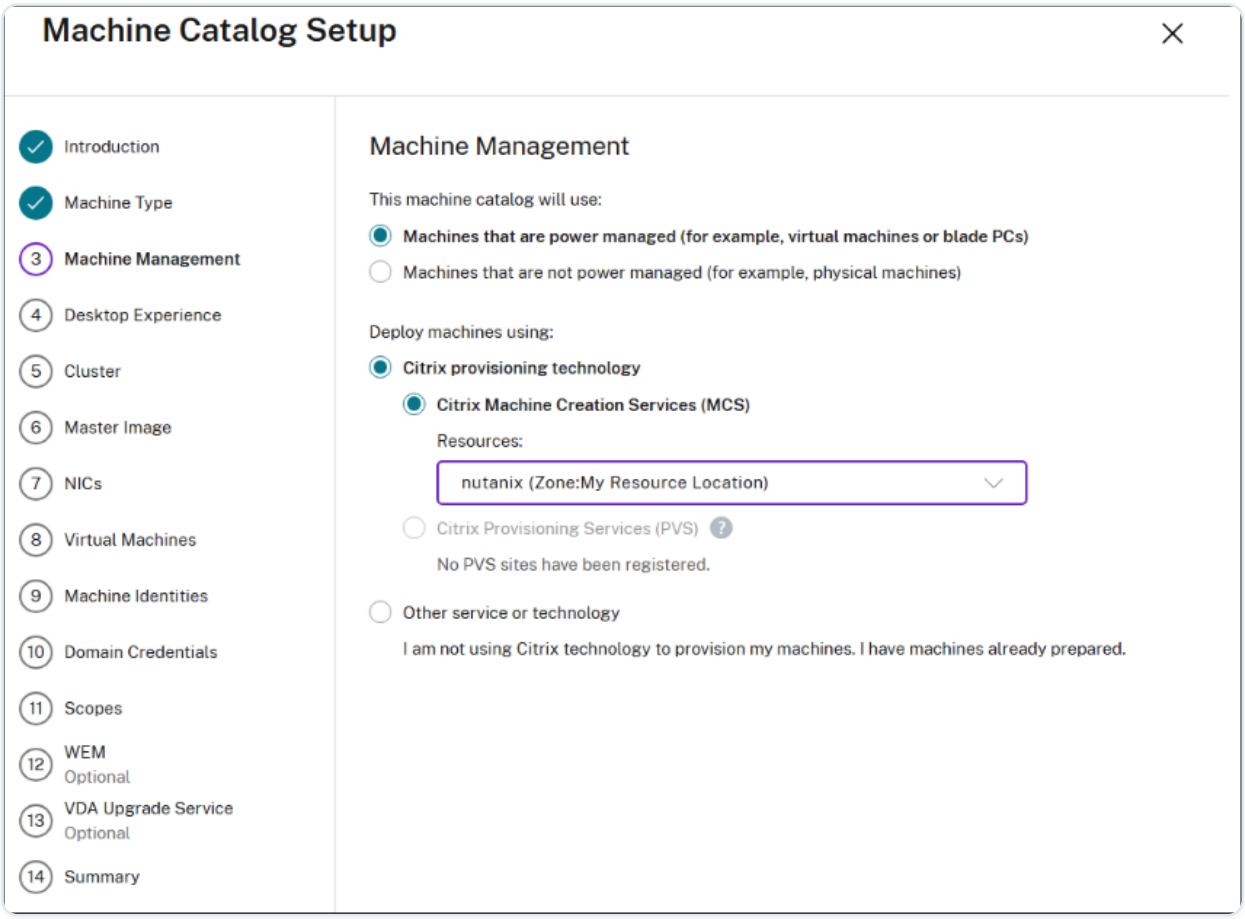
- Attaching multiple NICs to the same subnet is not supported.
- Due to Nutanix limitation, each MCS provisioned machine catalog can only be assigned with NICs in a single type of network among Overlay networks, VLAN Basic Subnets, and VLAN Subnets.
- In some scenarios, updating MCS master image for a non-persistent machine catalog might cause potential issues. See Secure Boot and vTPM in Nutanix Prism Central.
- When creating a machine catalog on Nutanix, cluster name containing a period (.) is not supported.
- When selecting a Nutanix VM template as the master image, the template name or template version name must not contain any characters like # or **&**.

Create a machine catalog using Studio

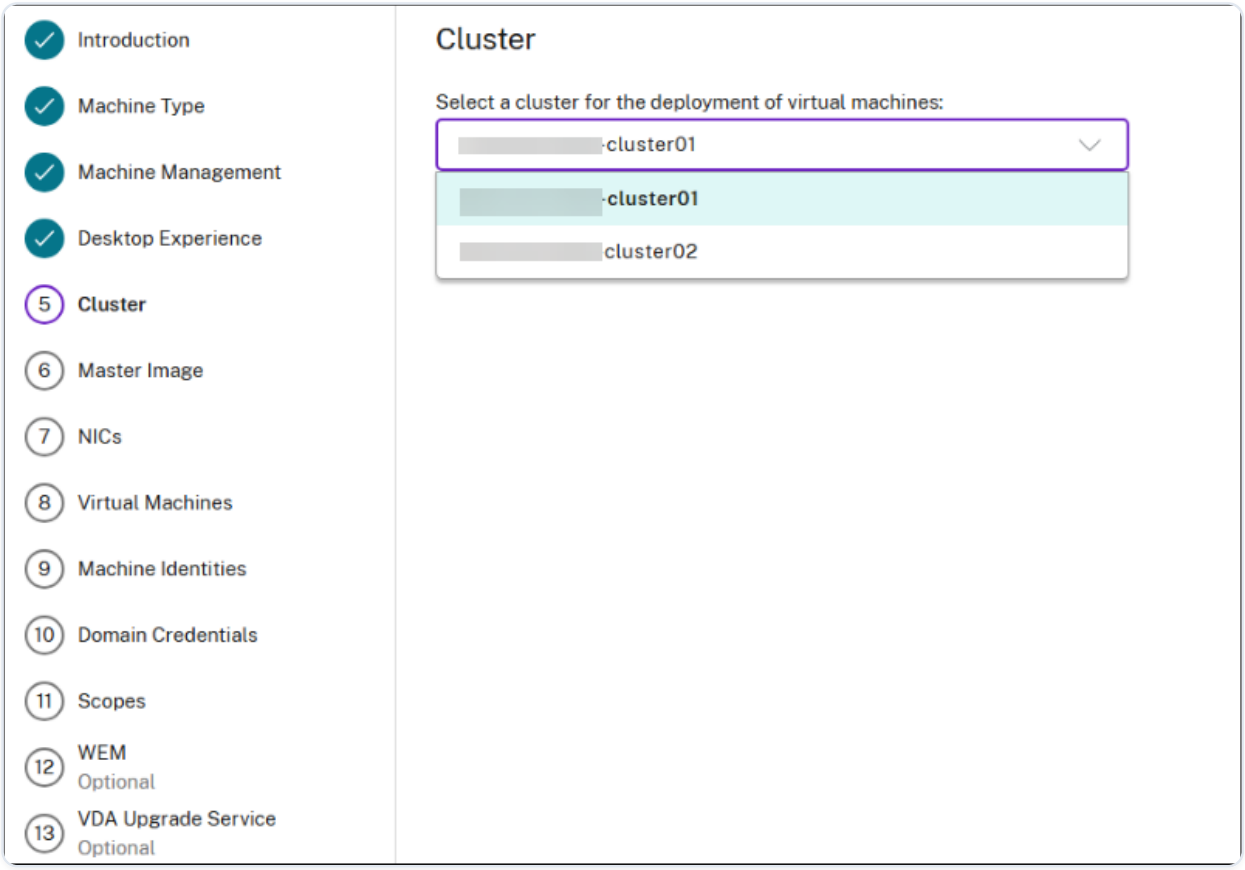
In the Machine Catalog Setup wizard:

1. On the **Machine Type** page, select **Multi-session OS**, **Single-session OS**, or **Remote PC Access**.
2. On the **Machine Management** page, select **Machines that are power managed** and **Citrix Machine Creation Services™** as the deployment method. Select the **Resources**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. On the **Desktop Experience** page, select one of the two options.
4. On the **Cluster** page, select a cluster for the deployment of the VMs.

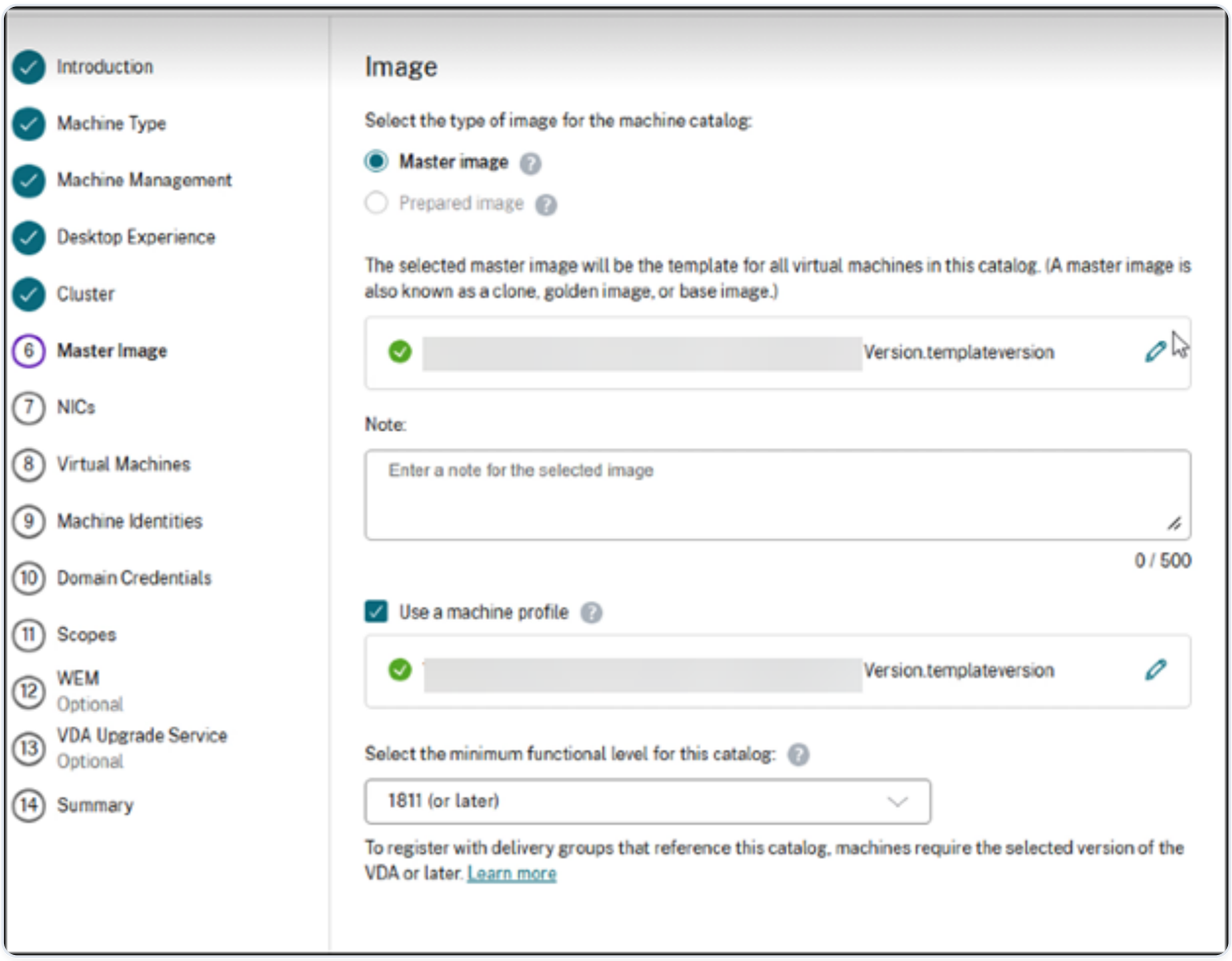


© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. On the **Master Image** page, click **Master Image** and select a master image (template version). You can filter machine templates by name. The master image's template version defaults as the machine profile for new catalogs. However, you can change the template version for the machine profile.

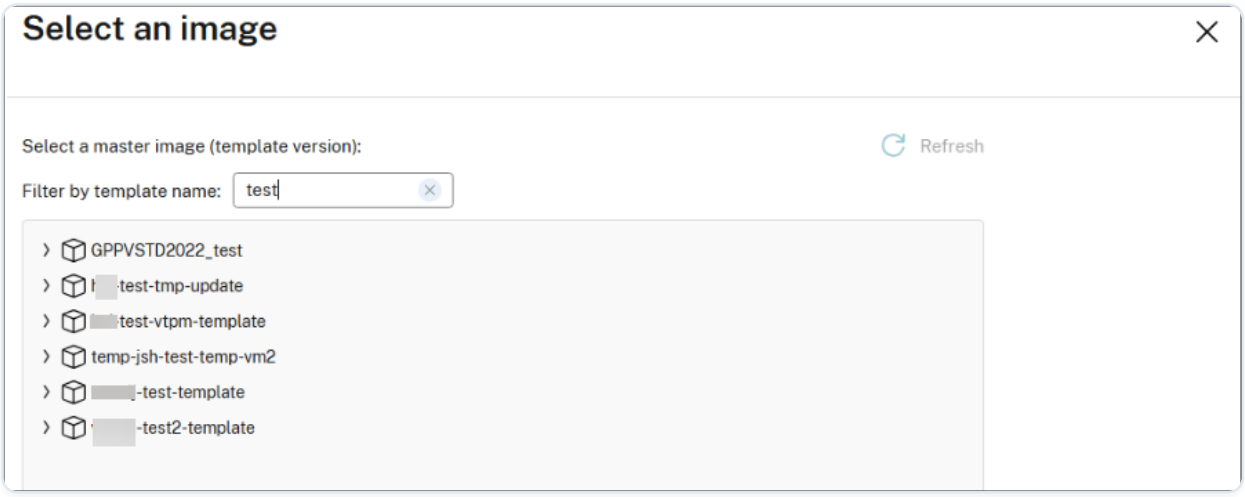
NOTE:

You can use a single Nutanix VM template version as the master VM for multiple MCS machine catalogs, even if those catalogs are on different Nutanix clusters.

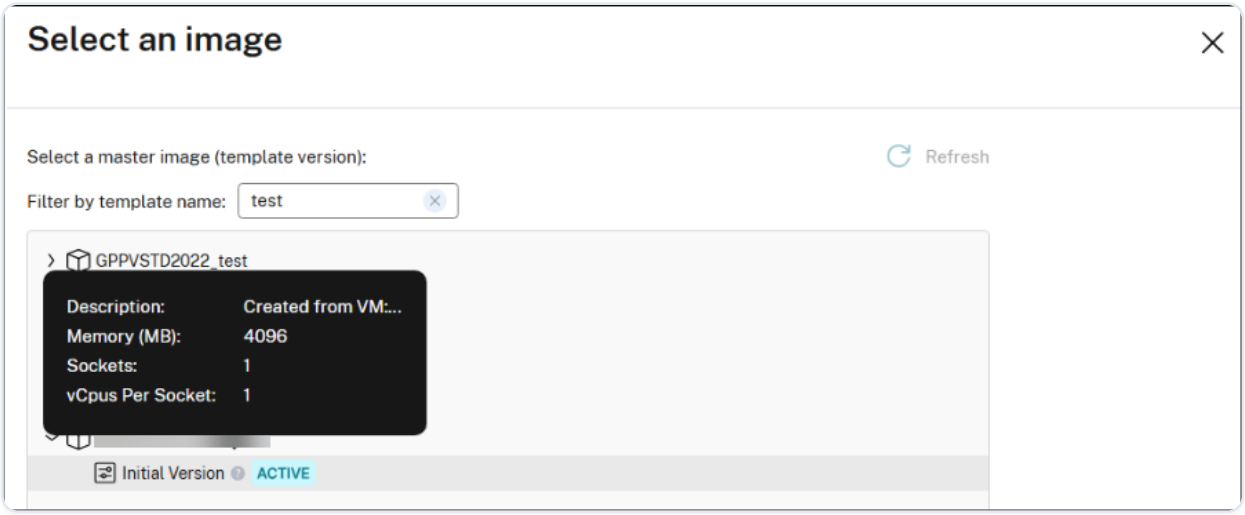


Filter machine templates by name:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



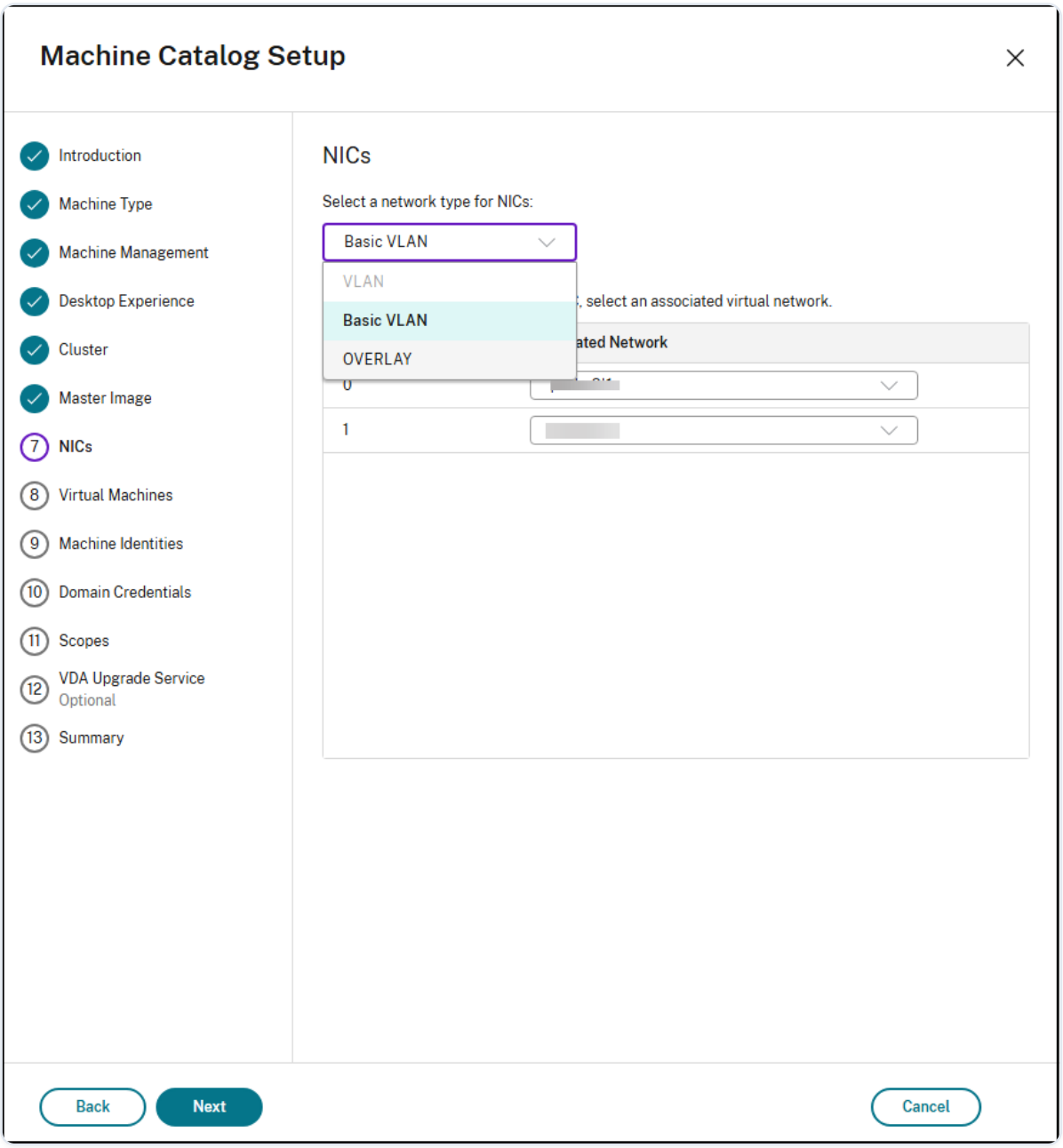
See description of a template:



6. On the **NICs** page:

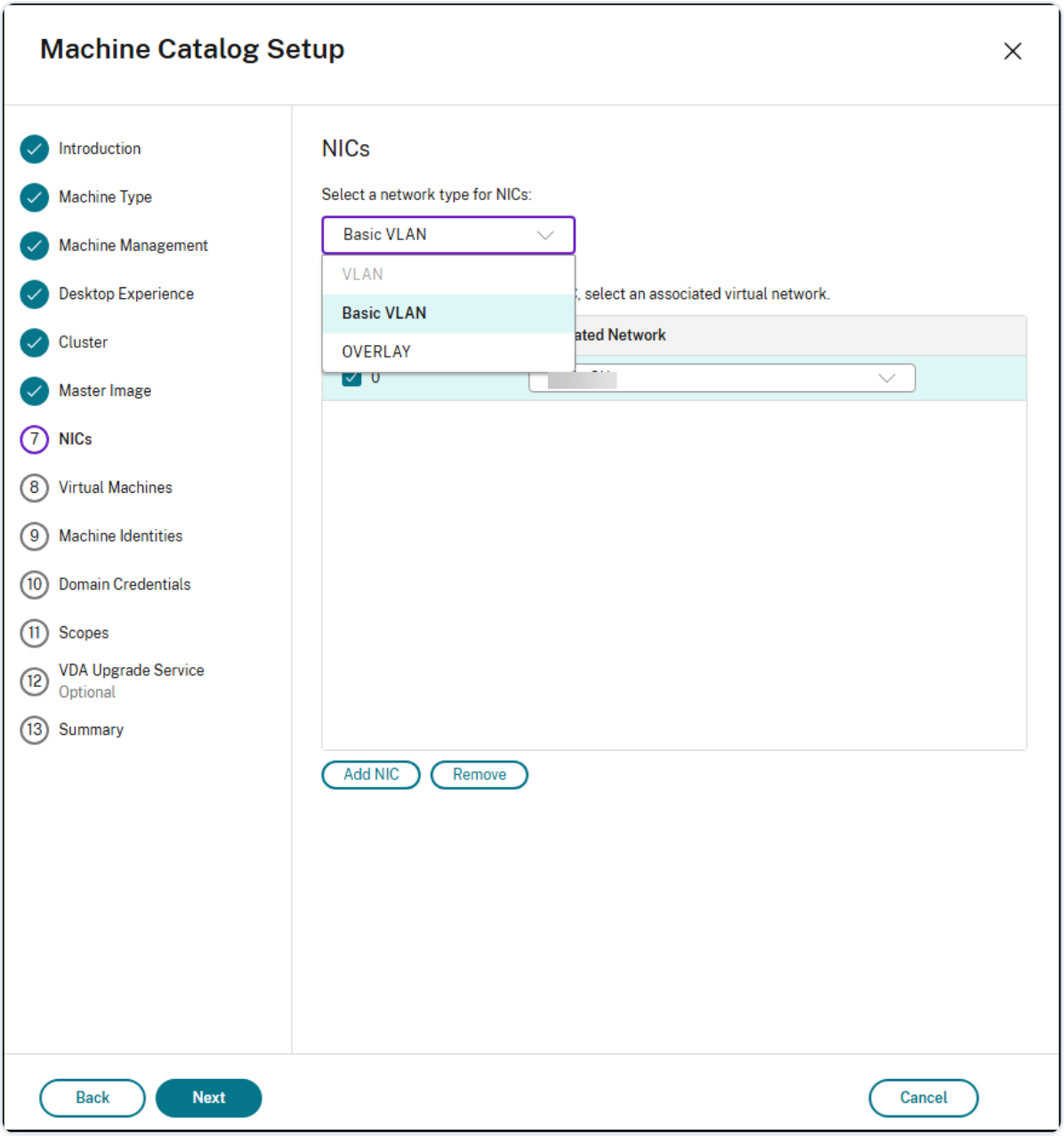
   - Select a NIC type from the drop-down to filter associated networks. The network types of NICs available are: **VLAN** (Advanced VLAN), **Basic VLAN**, and **OVERLAY**.
   - If you create a catalog with a machine profile, then the NIC number is consistent with the NIC number of the machine profile and can't be changed. Select an associated virtual network for each NIC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- If you create a catalog without a machine profile, click **Add NIC** to increase NIC count or click **Remove** to delete selected NICs. Select one or more NICs and then select an associated virtual network for each NIC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. On the **Virtual Machines** page, indicate the number of virtual machines you want to create and configure your machines for Total memory (MB) on each machine, Virtual CPUs, and Cores per CPU. These values are automatically populated from the machine profile.
8. On the **Summary** page, check the details of the machine catalog. Enter a name and description for the machine catalog. Click **Finish**.

EXPORT THE MACHINE PROFILE

You can export the machine profile used by the machine catalog to a JSON file.

1. Select the machine catalog and navigate to the **Templates Properties** tab.
2. Under **Machine Profile** details, click **Export** next to the **Last version**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a machine catalog using PowerShell commands

1. Open the PowerShell window.
2. Run `asnp citrix*`.
3. Create an identity pool if not already created. For example:

```
New-AcctIdentityPool    -Domain "<string>" -IdentityPoolName "<string>"
-IdentityType "ActiveDirectory"  -NamingScheme "DemoVM-##"
-NamingSchemeType "Numeric" -ZoneUid "GUID" -Scope @()
```

4. Create a provisioning scheme.

   For example: Without a machine profile

```
New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"ClusterId`"
Value=`"00062c63-1fb0-58c9-4fc8-5c2573352378`" /><Property
xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>" -HostingUnitName "<Hosting unit name>"
-IdentityPoolName "<string>" -InitialBatchSizeHint 1  -MasterImageVM
"XDHyp:\HostingUnits\<Hosting Unit Name>\Templates.folder\<template
name>.template\<template version name>.templateversion" -NetworkMapping
@{"5"="XDHyp:\HostingUnits\<Hosting unit name>\Clusters.folder\<Cluster
Name>.cluster\<Network name>.network"} -ProvisioningSchemeName
"<Catalog name>" -ProvisioningSchemeType "MCS" -RunAsynchronously
-Scope @() -VMCpuCount 2 -VMMemoryMB 10240
```

   For example: With a machine profile

   Use a machine profile to capture hardware properties from a template version and apply them to provisioned VMs. If you don’t specify machine profile, hardware properties are captured from the master image template version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- The OS Disk, vTPM, and Secure Boot properties are always captured from the master image, even when a machine profile is used.
- Since OS Disk is not read from the machine profile, you can create a diskless VM and convert it to a template version that can be used for the machine profile.
- As the complete JSON spec of the machine profile template version is stored, you can create the VMs even if you delete the template version from the Prism Central.

Properties captured from the machine profile are:

PROPERTY	PROPERTY NAME IN API (GETTEMPLATEVERSIONBYID)	COMMENTS/REFERENCES
CPU	**numSockets**	
RAM	**memorySizeBytes**	
Core	**numCoresPerSocket**	
Categories	**categories**	Category Management
GPU	**gpus**	GPUs Summary View
Threads Per Core	**numThreadsPerCore**	aCLI-VM
Numa Nodes	**numNumaNodes**	
Enable VCPU Hard Pinning	**isVcpuHardPinningEnabled**	
Enable CPU Passthrough	**isCpuPassthroughEnabled**	
Enable Memory Overcommit	**isMemoryOvercommitEnabled**	Creating a VM through Prism Central (AHV)
Enable GPU Console Access	**isGpuConsoleEnabled**	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PROPERTY	PROPERTY NAME IN API (GETTEMPLATEVERSIONBYID)	COMMENTS/REFERENCES
Enable CPU Hot Plug	**isCpuHotplugEnabled**	
Enable SCSI Controller	**isScsiControllerEnabled**	
Timezone	**hardwareClockTimezone**	Creating a VM through Prism Central (AHV)
Enable AHV branding	**isBrandingEnabled**	
Enable VGA Console	**isVgaConsoleEnabled**	
VM	**isAgentVm**	Creating a VM through Prism Central (AHV)

NOTE:

Using the same master image template version, you can create different catalogs with various machine profiles, each featuring a distinct set of properties mentioned above. For example, you might assign different Categories that can be linked to Nutanix Policies, adjust CPU/Memory, modify Memory Overcommit settings, or add and remove multiple GPUs.

The command-line parameters, such as `VMCpuCount`, `VMMemoryMB`, and `CPUCores` in the `CustomProperties`, can be provided and takes precedence over the values for these parameters from the machine profile template version. If not provided, these are read from the given machine profile.

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

    <StringProperty Name="CPUCores" Value="2" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</CustomProperties>

"@



New-ProvScheme -HostingUnitName "<Hosting unit name>" `

           -IdentityPoolName "<string>" `

           -InitialBatchSizeHint 1 `

           -MasterImageVM "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name>.template\<template version
name>.templateversion" `

           -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name for machine
profile>.template\<template version name>.templateversion" `

           -NetworkMapping @{"0"="XDHyp:\HostingUnits\<Hosting unit
name>\Clusters.folder\<Cluster Name>.cluster\<Network name>.network"} `

           -ProvisioningSchemeName "<Catalog name>" `

           -ProvisioningSchemeType "MCS" `

           -CustomProperties $customProperties `

           -RunAsynchronously `

           -VMCpuCount 2 `

           -Scope @()
```

5. Register a provisioning scheme as a broker catalog. For example:

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False  -
MinimumFunctionalLevel "L7_20" -Name "<Catalog Name>"
-PersistUserChanges "Discard" -ProvisioningType "MCS"    -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
SessionSupport "MultiSession" -ZoneUid "GUID"  -ProvisioningSchemeId
fe7df345-244e-4xxxx-xxxxxxxxx `  -Scope @()
```

Create a machine catalog with existing machines (power managed)

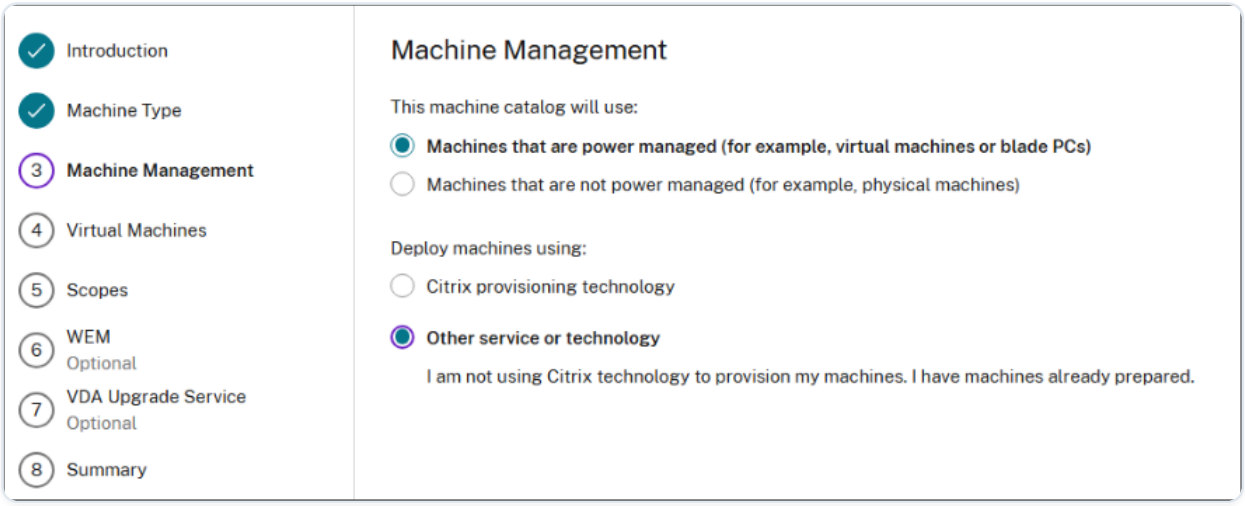
You can create a machine catalog with existing machines (power managed) using:

- Studio
- PowerShell

Create a machine catalog with existing machines (power managed) using Studio

In the Machine Catalog Setup wizard:

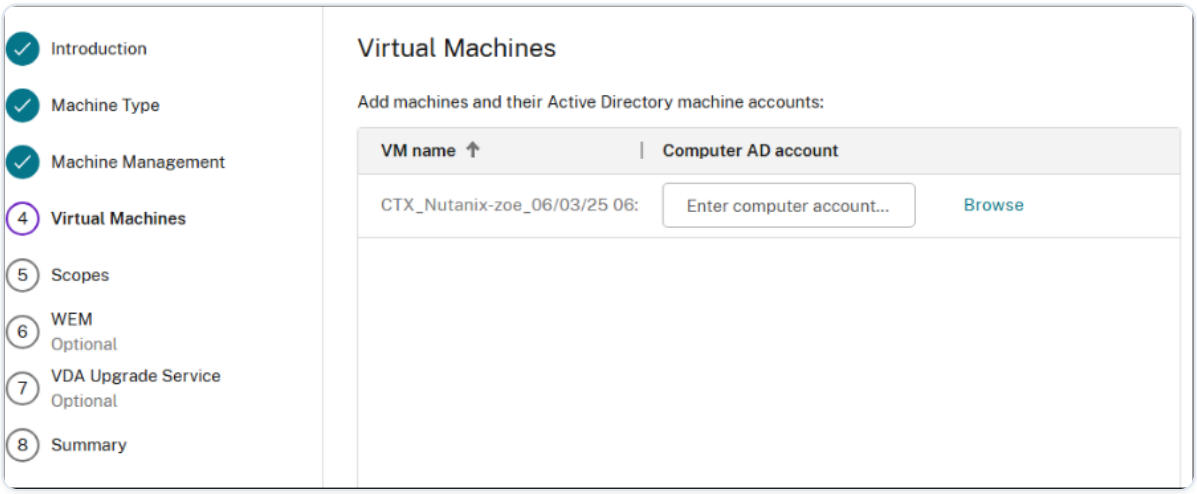
1. On the **Operating System** page, select **Multi-session OS** or **Single-session OS**.
2. On the **Machine Management** page, select **Machines that are power managed** and **Other service or technology**.



3. On the **Virtual Machines** page, add machines and their Active Directory machine accounts. You can do one of the following:

   - Click **Import from CSV file** to bulk add machines. For information about using CSV files to add machines, see Use CSV files to bulk add machines to a catalog.
   - Click **Add Machines** to add machines manually. The **Select VMs** window appears. Expand the Nutanix AHV Prism Central connection that you created earlier and select the VMs you want to add. Then add the associated machine account names.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. The **Scopes** and **Summary** pages do not contain information specific to Nutanix AHV Prism Central.

Create a machine catalog with existing machines (power managed) using PowerShell

1. Open the PowerShell window.
2. Run `asnp citrix*`.
3. Create a catalog to have power-managed VMs that are assigned to the user. For example:

```
New-BrokerCatalog -AllocationType "Permanent"  -IsRemotePC $False
-MachinesArePhysical $False  -Name "<Catalog Name>" -PersistUserChanges
"OnLocal" -ProvisioningType "Manual" -Scope @() -SessionSupport
"SingleSession" -ZoneUid "fb202053-8c35-4db2-a299-a8d9538ec6be"
```

4. Add VMs to the catalog. For example:

```
New-BrokerMachine  -CatalogUid 6 -HostedMachineId "d859caf3-4bf0-447b-
b012-8af0594c7d88" -HypervisorConnectionUid 1 -IsReserved $False  -
MachineName "S-1-5-21-1334627847-1250330507-3910179295-100245"
```

Create a machine catalog using a Nutanix snapshot

This section describes how to create an MCS provisioned machine catalog with Nutanix Acropolis (Prism Element) host connection. Before creating the catalog, create master images and snapshots in Nutanix. For more information, see the Nutanix documentation.

In the Machine Catalog Setup wizard:

- The **Container** or **Cluster and Container** page is unique to Nutanix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - If you deploy machines by using Nutanix AHV XI as the resources, on the **Container** page, select a container where the VMs' identity disks will be placed.
    - If you deploy machines by using Nutanix AHV PC as the resources, you see the **Cluster and Container** page. Select which cluster to use for the deployment of VMs and then a container.

- On the **Image** page, select the image snapshot. Use the Acropolis console to rename your snapshots if needed. If you rename snapshots, restart the catalog creation wizard to see a refreshed list.
- On the **Virtual Machines** page, indicate the number of virtual CPUs and the number of cores per vCPU.
- On the **NICs** page, select the NIC type to filter associated networks. This option is available only for Nutanix AHV PC connections.
- The **Machine Identities**, **Domain Credentials**, **Scopes**, and **Summary** pages do not contain Nutanix-specific information.

Limitations

When creating an MCS catalog with Nutanix host connection (specifically, Nutanix AHV plug-in 2.7.1 and Nutanix AHV plug-in 2.5.1), the hard disk size of provisioned VMs are incorrectly displayed on Studio.

- Nutanix AHV plug-in 2.7.1: The size displayed is smaller (1 GB) than the real storage size.
- Nutanix AHV plug-in 2.5.1: The size displayed is smaller (32 GB) than the real storage size.

However, this works as designed if the master image VM is a snapshot in VM.

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a Nutanix catalog.

More information

- Create and manage connections and resources
- Connection to Nutanix
- Connection to Nutanix cloud and partner solutions
- Create machine catalogs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a Red Hat OpenShift catalog

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Red Hat OpenShift virtualization environments.

NOTE:

Before creating a Red Hat OpenShift catalog, finish creating a connection and hosting unit to Red Hat OpenShift. See Connection to Red Hat OpenShift.

Create a master image VM

A master image VM is required to create a machine catalog.

1. Access the OpenShift Console using your login ID.
2. Navigate to **Virtualization > VirtualMachines** to see the list of VMs, including master image VMs.
3. Create a master image. When creating a master image, make sure that the master image VM has only one storage device.

NOTE:

- Ensure that a routable NAD is added to the master image VM according to the customer's requirements for the cluster environment.
- When the master image is joined to a domain, it might lose domain trust after being used for catalog creation. This issue affects Citrix Virtual Apps and Desktops™ 2503 due to a limitation in the OpenShift environment. The workaround is not to join domain in master images. Citrix is working with Red Hat to enhance network isolation capabilities.
- When creating an MCS machine catalog in a Red Hat OpenShift virtualization environment, you can’t use a master image and a machine profile that have different operating system types. This is due to how Red Hat OpenShift manages each OS type. Therefore, using a Windows VM as the master image with a non-Windows (example, Linux) VM as the machine profile, or the other way around, is not supported.
- Currently, the VMs created using `InstanceType` are not supported as a master image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a catalog

You can create OpenShift catalogs to create, deliver, and power manage machines in your OpenShift environments.

- Create a catalog using Studio
- Create a catalog using PowerShell commands

Create a catalog using Studio

You can create an MCS machine catalog in the Red Hat OpenShift environment with or without a machine profile using Web Studio. A VM is used as a machine profile input.

In the Machine Catalog Setup wizard:

1. On the **Operating System** page, select **Multi-session OS** or **Single-session OS**.
2. On the Machine Management page:
    - Select **Machines that are power managed (for example, virtual machines or blade PCs)**.
    - Select to deploy machines using **Citrix provisioning technology Citrix Machine Creation Services™ (MCS)**.
    - Select the Openshift hosting unit under Citrix Machine Creation Services (MCS)
3. On the **Desktop Experience** page, select the option according to the machine type you select on the **Machine Type** page.
4. On the **Image** page:
    a. Select a master image. Currently, Openshift doesn’t support Prepared image.
    b. You can add a note for the selected image.
    c. You can select the **Use a machine profile** checkbox and select a machine profile.
    d. To enable use of the latest product features, ensure that the master image has the latest VDA version installed. Do not change the default minimum VDA selection. However, if you must use an earlier VDA version, see VDA versions and functional levels.
5. On the **NICs** page, select one or more NICs, associate a virtual network with each card.
6. On the **Virtual Machines** page:
    a. Specify how many virtual machines to create. Enter 0 (zero) if you do not want to create any. Later, you can create VMs for an empty catalog by adding machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Choose the amount of memory (in MB) each VM has.

c. If you are creating a random non-persistent catalog, you can enable Write-Back Cache for machines to improve I/O performance. See Configure cache for temporary data.

7. Follow the on-screen instructions to complete the remaining steps, which don't include OpenShift-specific information.

You can also use Studio to create Openshift catalogs to deliver and manage the power of existing machines in your OpenShift environments. Do the following:

In the Machine Catalog Setup wizard:

1. On the **Operating System** page, select **Multi-session OS** or Single-session OS.
2. On the **Machine Management** page, select **Machines that are power managed and Another service or technology**.
3. On the **Virtual Machines** page, add machines and their Active Directory machine accounts. You can:

   - *Add machines manually*: Click **Add Machines to add machines manually**. The **Select VMs** window appears. Expand the OpenShift connection you created earlier and select the nodes (VMs) you want to add. Then add the associated machine account names.
   - *Add machines using a CSV file*: Click **Add CSV File to bulk add machines**. For information about using CSV files to add machines, see Use CSV files to bulk add machines to a catalog.

4. Follow the on-screen instructions to complete the remaining steps, which don't include OpenShift-specific information.

Create a catalog using PowerShell commands

Currently, you can create an MCS machine catalog in the Red Hat OpenShift environment using only PowerShell commands. You can create the machine catalog with or without using a machine profile. A VM is used as a machine profile input.

1. Open a PowerShell window.
2. Run `asnp citrix*`.
3. Run PowerShell commands to

   a. Create an identity pool

   b. Create AD accounts

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Create an MCS machine catalog with persistent VMs with or without a machine profile.
d. Add VMs to the catalog
e. Create a broker catalog
f. Add broker machines to the new VMs

Following is a sample script:

CREATE AN IDENTITY POOL

```
New-AcctIdentityPool `

    -IdentityPoolName "IdentityPoolName" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -NamingScheme "vm###" `

    -NamingSchemeType "Numeric" `

    -AllowUnicode `

    -Domain "MyDomain.local" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

CREATE AD ACCOUNTS

```
New-AcctADAccount `

    -IdentityPoolUid "11111111-1111-1111-1111-111111111111" `

    -ADUserName "MyDomain\MyUserName" `

    -ADPassword SecurePassword `

    -Count 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CREATE A PROVISIONING SCHEME WITH PERSISTENT MACHINES (WITHOUT MACHINE PROFILE)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

CREATE A PROVISIONING SCHEME WITH PERSISTENT MACHINES (WITH MACHINE PROFILE)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local" `

    -MachineProfile "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MachineProfileVM.v
m"
```

CREATE NEW PROVVMS

```
New-ProvVM `

    ProvisioningSchemeName "ProvisioningSchemeName" `

    ADAccountName "MyDomain\vm001" `

    AdminAddress "MyDDC.MyDomain.Local"



Lock-ProvVM `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -Tag "Brokered" `

    -VMID "TargetNamespace:vm001"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CREATE NEW BROKER CATALOG

```
New-BrokerCatalog `

    -Name "ProvisioningSchemeName" `

    -ProvisioningType "MCS" `

    -SessionSupport "MultiSession" `

    -AllocationType "Random" `

    -PersistUserChanges "OnLocal" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

SET BROKER CATALOG METADATA

```
Set-BrokerCatalogMetadata `

    -CatalogId "1" `

    -Name "Citrix_DesktopStudio_IdentityPoolUid" `

    -Value "11111111-1111-1111-1111-111111111111"



Set-BrokerCatalog `

    -Name "ProvisioningSchemeName " `

    -ProvisioningSchemeId "22222222-2222-2222-2222-222222222222"
```

CREATE BROKER MACHINES FOR THE NEW PROVVMS

```
New-BrokerMachine `

    -CatalogUid "33333333-3333-3333-3333-333333333333" `

    -AdminAddress "MyDDC.MyDomain.Local" `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    -MachineName "S-0-0-00-0000000000-0000000000-000000000-000000"
```

Where to go next

- If this is the first catalog created, Studio guides you to Create a delivery group

More information

- Create and manage connections and resources
- Connection to Red Hat OpenShift
- Create machine catalogs

Create a VMware catalog

Create machine catalogs describes the wizards that create a machine catalog.

NOTE:

Before creating a VMware catalog, you need to finish creating a connection to VMware. See Connection to VMware.

Create a machine catalog using a machine profile

You can create an MCS machine catalog using a machine profile. The source of the machine profile input is a VMware template. The machine profile captures the hardware properties from a VMware template and applies them to the newly provisioned VMs in the catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Master image input (snapshot) and machine profile input (VMware template) must either be both vTPM enabled or both vTPM disabled. This rule applies to both `New-ProvScheme` and `Set-ProvScheme`.
- If the master image is vTPM enabled, then the VMware template can only come from the same VM source as the master image.
- Encrypted storage policy only supports full clone.
- The machine profile-based catalogs utilize the provided VMware template to gather storage controller information, relying on the attached virtual disks. The template must include a virtual disk which is required to retrieve the storage controller information that is used to configure virtual disks for the virtual machines.

The VMware template in the machine profile must exist during the catalog life cycle to allow provisioning of VMs to the catalog. Without a VMware template, you cannot provision new VMs. When a VMware template gets deleted, you must supply a new template using the `Set-ProvScheme` command.

- MCS captures the properties of a VMware template. You can create a new VMware template referencing stored properties of the VMware template using the `Get-Provscheme` command.
- Alternatively, if the machine catalog and provisioned VMs exist, then an MCS provisioned machine can also be used to create a new VMware template.
- When MCSIO is enabled, you can update the memory and disk cache sizes after creating the MCS catalogs.

Based on different OS, you can create a machine catalog with different configurations:

- If Windows 11 is installed on the master image, then it is a requirement to have vTPM enabled for the master image. Therefore, the VMware template, which is a source of machine profile, must have vTPM attached to it.
- If Windows 10 is installed on the master image with no vTPM attached, then you can create a machine catalog with non-vTPM VMware template as source for machine profile.

There is another configuration where you can create a machine catalog using full copy disk mode with machine profile template applied with encrypted storage policy.

To create a machine catalog using PowerShell commands with machine profile as input:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run the following commands:

   - To create a machine catalog with vTPM attached VMware template as a source for machine profile input and windows11 installed master image:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4  -VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<catalog name>"
-ProvisioningType 'MCS'

-Scope @()  -SessionSupport "SingleSession"

-ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- To create a machine catalog with non-vTPM VMware template as source for machine profile and Windows10 installed master image:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "<string>"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"  -Description "<string>"  -IsRemotePC
$False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()  -SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- To create a machine catalog using Full copy disk mode with machine profile template applied with encrypted storage policy:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"

-UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- To update a machine profile, use the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName
'name' -MachineProfile 'XDHyp:\HostingUnits\<hosting unit
name>\<template name>.template
```

Check for multiple NICs

You get various error messages during the pre-flight checks for multiple NICs when using a machine profile and the `NetworkMapping` parameter in the `New-ProvScheme` and `Set-ProvScheme` commands.

The pre-flight checklist for multiple NICs is as follows:

- Only NIC count from the machine profile template is used and validated. The network to which these NICs point towards, is not used or validated against the hosting unit networks.
- If the NIC count in the machine profile template is greater than the number of networks in the hosting unit, you get an error message.
- If the NIC count in the machine profile template is zero, you get an error message. When the NIC count in the machine profile template is one, then:
  - If no network mapping is specified in the `New-ProvScheme` or `Set-ProvScheme` command, and the hosting unit network is one, then the hosting unit network is used.
  - If a network mapping is specified, then the specified network mapping is used if it is valid.
- When the NIC count in the machine profile template is greater than 1, or the hosting unit network count is greater than 1, then:
  - Valid network mapping is required in the command, and it should provide mapping for each NIC (that is, the NetworkMapping count must be the same as the machine profile NIC count).
  - Multiple NICs cannot be mapped to the same network in the hosting unit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `NetworkMapping` count and machine profile NIC count must be less than or equal to the hosting unit network count.
- `NetworkMapping` must be provided for each id from 0 to n-1, where n is the number of network adapters in the machine profile template.

Provision a Data disk on MCS created VM

A Data disk allows storage of persistent data like event logs, security traces, and application data. You can create and assign a persistent or non-persistent Data disk to an MCS created persistent or non-persistent VM of an MCS machine catalog in VMware.

Provision the Data disk from the master image. The prepared master image Data disk is stored in `<Prov Scheme Name>-dataDisk-<datastoreId>` folder.

You can create both machine profile and non-machine profile-based MCS catalog. For machine profile-based MCS catalog, you can use the same master image VM as the Data disk source for the machine profile.

The provisioned VM's Data disk derives properties like storage policy and size from the master image. For machine profile based catalog, it can optionally use the VM template's Data disk for deriving the properties. If the VM template doesn't have a data disk, then Storage's default policy is used.

The Data disk of the provisioned VM is created in the same directory as the OS and Identity disk.

Supported Data disk scenarios

Following are the supported OS disk and Data disk scenarios:

- Persistent OS disk with persistent Data disk
- Non-persistent OS Disk with persistent Data disk
- Non-persistent OS Disk with non-persistent Data disk

NOTE:

A persistent machine catalog cannot have a non-persistent Data disk.

Limitations

The following operations are currently not supported:

- Provisioning of more than one Data disk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Resetting the Data disk.
- Updating an MCS catalog with a Data disk to a non-Data disk MCS catalog. Similarly, updating an MCS catalog without a Data disk to a Data disk MCS catalog.

Key steps

1. Create a master image VM with a Data disk in VMware. For a machine profile-based MCS catalog, you can use the same master image VM as the Data disk source for the machine profile.
2. Create an MCS machine catalog with Data disk provisioned VMs using the `New-ProvScheme` PowerShell command. See Create a catalog with Data disk provisioned VMs.
3. Add VMs to the catalog using the `New-ProvVM` PowerShell command.
4. Log in to the VM to see if the Data disk is formatted correctly. If there is content on the Data disk referenced in the master image VM, then that content is also on the Data disk.

Create a master image VM with Data disk in VMware

1. Create a VM with two hard disks. One is the OS disk and second is the Data disk. Follow this guide to add a New Hard Disk (Data disk) to an existing VM.
2. Log in to the VM to initialize the disk, set the desired drive letter, and add the content.

Create a catalog with Data disk provisioned VMs

Include the following parameters in the `New-ProvScheme` PowerShell command to provision an MCS machine catalog with Data disk.

- `DataDisk`: To Specify the path of the Data disk specified.
- `DataDiskPersistence`: To indicate whether the DataDisk is persistent or non-persistent.

  The Data disk cannot be non-persistent if `CleanOnBoot` is false. You cannot change the value of `DataDiskPersistence` for a machine catalog once configured.

After you create the catalog, add VMs using the `New-ProvVM` command.

Image update

Run `Publish-ProvMasterVMImage` command to update the source of the OS and Data disk. After running the `Publish-ProvMasterVMImage` command:

- The new VMs are created with the updated OS and Data disks.
- The existing VMs' non-persistent disks are updated on the next power cycle.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The existing VMs' persistent disks are not updated on the next power cycle.

Delete the Data disk

If you delete the catalog, the Data disk is deleted unless you use `forgetVM` or `purgeDBOnly` option. If you delete the VM, the Data disk is deleted unless you use the `forgetVM` or `purgeDBOnly` option. These conditions are applicable to only persistent MCS machine catalogs.

Troubleshooting

If the catalog fails to create, see CTX294978.

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a VMware catalog.

More information

- Create and manage connections and resources
- Connection to VMware
- Connection to VMware cloud and partner solutions
- Create machine catalogs

Create a XenServer® catalog

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to XenServer (formerly Citrix Hypervisor) virtualization environments.

NOTE:

Before creating a XenServer catalog, you need to finish creating a connection to XenServer. See Connection to XenServer.

Create a machine catalog using a GPU-capable XenServer

GPU-capable machines require a dedicated master image. Those VMs require video card drivers that support GPUs. Configure GPU-capable machines to allow the VM to operate with software that uses the GPU for operations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In XenCenter®, create a VM with standard VGA, networks, and vCPU.
2. Update the VM configuration to enable GPU use (either Passthrough or vGPU).
3. Install a supported operating system and enable RDP.
4. Install Citrix VM Tools and NVIDIA drivers.
5. Turn off the Virtual Network Computing (VNC) Admin Console to optimize performance, and then restart the VM.
6. You are prompted to use RDP. Using RDP, install the VDA and then restart the VM.
7. Optionally, create a snapshot for the VM as a baseline template for other GPU master images.
8. Using RDP, install customer-specific applications that are configured in XenCenter and use GPU capabilities.

Create a machine profile-based machine catalog using PowerShell

When you create a catalog to provision machines using MCS, you can use a machine profile to capture the hardware properties from a virtual machine and apply them to newly provisioned VMs in the catalog. If the `MachineProfile` parameter is not used, the hardware properties are captured from the master image VM or snapshot.

You can also create an MCS machine catalog using a machine profile that is enabled with vTPM. This helps to create machine catalogs of Windows 11 VMs with vTPM enabled.

NOTE:

- Currently, you can use only a snapshot as a machine profile input.
- If master image input is vTPM enabled, then the machine profile input must also be vTPM enabled. This rule applies to both `New-ProvScheme` and `Set-ProvScheme`.
- If the master image is vTPM enabled, then the machine profile can only come from the same VM source as the master image.
- On catalog creation, the vTPM of the VM should be the same vTPM that is in use for the master image snapshot.

You can update the memory and disk cache sizes after creating the MCS catalogs when MCSIO is enabled. You can explicitly configure the following parameters to overwrite the values of the parameters in the machine profile input:

- `VMCpuCount`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `VMMemory`
- `NetworkMapping`

Create a catalog with a machine profile

1. Open the PowerShell window.
2. Run `asnp citrix*`.
3. Create an identity pool. The identity pool is a container for the Active Directory (AD) accounts for the VMs to be created. For example:

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. Create the required AD computer accounts in Active Directory.

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. Run the `New-ProvScheme` command to create a catalog. For example:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm\ExampleSnapsh
ot.snapshot"
```

6. Register provisioning scheme as a broker catalog. For example:

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. Add VMs to the catalog.

Update a catalog with a new machine profile

NOTE:

- The `Set-ProvScheme` command in this case does not change the machine profile of the existing VMs in the catalog. Only the newly created VMs added to the catalog have the new machine profile.
- You cannot convert a machine profile-based machine catalog to non-machine profile-based machine catalog.

To update a catalog with a new machine profile:

1. Run the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

   For more information on the Set-ProvScheme command, see Set-ProvScheme.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Where to go next

- If this is the first catalog created, you are guided to create a delivery group.
- To review the entire configuration process, see Plan and build a deployment.
- To manage catalogs, see Manage machine catalogs and Manage a XenServer catalog.

More information

- Create and manage connections and resources
- Connection to XenServer
- Create machine catalogs

Identity pools of different machine identity join types

Using MCS, you can provision machines as non-domain-joined, on-premises AD joined, Microsoft Entra joined, or Microsoft Entra hybrid joined.

For information about how to configure machine identities in Studio, see Create machine catalogs.

For specific information on how to create identity pools of different machine identity join types, see the following:

- Identity pool of on-premises Active Directory joined machine identity
- Identity pool of Microsoft Entra joined machine identity
- Identity pool of Microsoft Entra hybrid joined machine identity
- Identity pool of Microsoft Intune enabled machine identity
- Identity pool of non-domain-joined machine identity

Identity pool of on-premises Active Directory joined machine identity

This article describes how to create identity pool of on-premises Active Directory joined machine identity using Citrix DaaS.

Use Studio

The following information is a supplement to the guidance in Create machine catalogs.

In the catalog creation wizard:

1. On the **Machine Identities** page:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Select identity type as **On-premises Active Directory**.

b. Select an Active Directory account option:

- **Create new Active Directory accounts**:
  - If you select **Create new Active Directory accounts** and do use an existing identity pool to create new accounts, then select a domain for those accounts and specify an account naming scheme.

    To find a specific domain quickly, type the domain name in the search box at the top of the **Location (domain)** dropdown and click **Enter**. **Web Studio** shows a progress indicator while it retrieves the matching domain.
  - If you select **Create new Active Directory accounts** and use an existing identity pool to create new accounts, then select an identity pool from the list.
- **Use existing Active Directory accounts**: You can browse or import from CSV file, and reset password or specify the same password for all accounts.

c. Click **Next**.

2. On the **Domain credentials** page, select a service account or enter credentials manually. For information on service accounts, see On-premises Active Directory service accounts.

Modify the service account association

To change the associated service account or add an association to an existing MCS machine catalog, use the **Edit Machine Catalog** page.

- To add a service account, click **Select service account** on the **Service Account** page.
- To change the service account association, click the edit icon on the **Service Account** page.

Use PowerShell

You can associate an on-premises service account with an MCS created machine catalog by associating an on-premises service account with the identity pool. You can create an identity pool or update an existing identity pool to associate it with a service account.

For example: To create a new identity pool and associate it with a service account, run the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-AcctIdentityPool -IdentityType ActiveDirectory -IdentityPoolName
MyPool -NamingScheme Acc#### -Domain MyDomain.com -NamingSchemeType
Numeric -OU "CN=MyOU,DC=MyDomain,DC=com" -ServiceAccountUid
$serviceAccountUid
```

For example: To update an existing identity pool to associate it with a service account, run the following:

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid

Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

NOTE:

The `$serviceAccountUid` must be a valid UID of an on-premises Active Directory service account.

More information

- Service accounts for machine identity management
- On-premises Active Directory service accounts

Identity pool of Microsoft Entra joined machine identity

This article describes how to create identity pool of Microsoft Entra joined machine identity using Citrix DaaS.

For information on requirements, limitations, and considerations, see Microsoft Entra joined.

Before you create the machine catalog, you need the following:

1. New resource location
    - Navigate to the Citrix Cloud™ admin UI > upper left hamburger menu > **Resource Locations**.
    - Click **+ Resource Location**.
    - Enter a name for the new resource location and click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Create a hosting connection. See Create and manage connections section for details. When deploying machines on Azure, see Connection to Azure Resource Manager.

You can create Microsoft Entra joined catalogs by using Studio or PowerShell.

Use Studio

The following information is a supplement to the guidance in Create machine catalogs. To create Microsoft Entra joined catalogs, follow the general guidance in that article, minding the details specific to Microsoft Entra joined catalogs.

In the catalog creation wizard:

1. On the **Image** page:
   - Select 2106 or later as the functional level.
   - Select **Use a machine profile** and select the appropriate machine from the list.
2. On the **Machine Identities** page:
   a. Select **Microsoft Entra joined**. The created machines are owned by an organization and are signed into with a Microsoft Entra account that belongs to that organization. They exist only in the cloud.

   NOTE:

   - The **Microsoft Entra joined** identity type requires version 2106 or later as the minimum functional level for the catalog.
   - The machines are joined to the Microsoft Entra domain associated with the tenant to which the hosting connection is bound.

   b. Click **Select service account** and select an available service account from the list. If a suitable service account is not available for the Microsoft Entra tenant that the machine identities will join to, you can create a service account. For information on service account, see Microsoft Entra service accounts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The service account that you selected might be in an unhealthy status due to various reasons. You can go to **Administrators > Service Accounts** to view details and fix the issues according to the recommendations. Alternatively, you can proceed with the machine catalog operation and fix the issues later. If you do not fix the issue, stale Microsoft Entra joined or Microsoft Intune enrolled devices are generated that can block Microsoft Entra join of the machines.

c. Click **Add Extension Attributes** to store unique, custom data directly on your Entra ID device objects. On the **Add Extension Attributes** page, add **Extension attributes** and **Value**.

NOTE:

- You can add a maximum of 15 extension attributes.
- The name must be unique and the value can't be empty.

d. Select an Active Directory account option:

- **Create new Active Directory accounts**:
  - If you select **Create new Active Directory accounts** and do use an existing identity pool to create new accounts, then select a domain for those accounts and specify an account naming scheme.
  - If you select **Create new Active Directory accounts** and use an existing identity pool to create new accounts, then select an identity pool from the list.
- **Use existing Active Directory accounts**: You can browse or import from a CSV file, and reset the password or specify the same password for all accounts.

- Specify an account naming scheme.

Users must be granted explicit access in Azure to log into the machines using their Microsoft Entra credentials. See Microsoft Entra joined section for more details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add or modify extension attributes

To change or add additional extension attributes to an existing MCS machine catalog, or add extension attributes to an MCS catalog without a service account, use the **Edit Machine Catalog** wizard.

- To change or add additional extension attributes, navigate to the **Microsoft Entra Device Extension Attributes** page. Click the pencil icon, and add or update extension attributes.
- To add extension attributes to an MCS catalog without a Microsoft Entra service account:

  a. Navigate to the **Service Account** page. Select a Microsoft Entra service account for the Microsoft Intra ID.

  b. Go to the Microsoft Entra Device Extension Attributes page, click **Add Extension Attributes**.

Modify the service account association

To change the associated service account or add an association to an existing MCS machine catalog, use the **Edit Machine Catalog** page.

- To add a service account, click **Select service account** on the **Service Account** page.
- To change the service account association, click the edit icon on the **Service Account** page.

Use PowerShell

The following are **PowerShell** steps equivalent to operations in Studio.

The difference between on-premises AD joined catalogs and Microsoft Entra joined ones lies in the creation of the identity pool and the provisioning scheme.

You must associate a Microsoft Entra service account with the identity pool, and then create the machine catalog. You can either create a new identity pool or update an existing identity pool to associate it with a service account.

Create new identity pool

For example: To create a new identity pool and associate it with a service account, run the following:

```
New-AcctIdentityPool -IdentityType AzureAD -IdentityPoolName MyPool
-NamingScheme Acc#### -NamingSchemeType Numeric -ServiceAccountUid
$serviceAccountUid
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example: To create a new identity pool with specified extension attributes and associate it with a service account, run the following:

```
New-AcctIdentityPool -IdentityPoolName MyPool -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType AzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

When a VM is powered on for the first time, after joining Microsoft Entra ID, the VM reports its Entra ID deviceId to MCS.

For example: To check the `EntraIDDeviceID`, run `Get-AcctADAccount` or `Get-AcctIdentity`.

```
Get-AcctADAccount -IdentityPoolName MyPool
```

After reboot, for persistent VMs, the `EntraIDDeviceID` remains the same. For non-persistent VMs, there is a new `EntraIDDeviceID` after every reboot.

NOTE:

MCS automatically removes associated extension attributes when you delete a VM from the catalog but don't delete from Azure.

Update existing identity pool

For example: To update an existing identity pool to associate it with a service account, run the following:

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid

Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

NOTE:

The `$serviceAccountUid` must be a must be a valid UID of a Microsoft Entra service account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example: To edit extension attributes for the existing catalog, run the following:

NOTE:

- After upgrading existing catalog VMs to VDA version 2511 or later, a reboot is necessary. This reboot allows the VM to report its Entra ID deviceId to MCS, enabling MCS to then configure the VM's extension attributes.
- The existing catalog should have an AzureAD type of service account with permission "Device.ReadWrite.All".

To add some new attributes:

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

To remove some existing attributes

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

OR

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` also updates the Entra ID device's extension attributes for VMs that are already joined to Entra ID and possess an `EntraIDDeviceID` value within their identities.

Create Microsoft Entra joined catalogs

To create a provisioning scheme for Microsoft Entra joined catalogs, the **MachineProfile** parameter is required in `New-ProvScheme`. For example:

```
New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"UseManagedDisks`" Value=`"true`" /><Property
xsi:type=`"StringProperty`" Name=`"StorageType`"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Value=`"StandardSSD_LRS`" /><Property xsi:type=`"StringProperty`"
Name=`"LicenseType`" Value=`"Windows_Server`" /></CustomProperties>"
-HostingUnitName "AzureResource" -IdentityPoolName "AzureADJoinedCatalog"
-InitialBatchSizeHint 1 -MachineProfile "XDHyp:
\HostingUnits\AzureResource\image.folder\azuread-
rg.resourcegroup\MasterVDA.vm" -MasterImageVM "XDHyp:
\HostingUnits\AzureResource\image.folder\azuread-rg.resourcegroup\azuread-
small_OsDisk_1_5fb42fadf7ff460bb301ee0d56ea30da.manageddisk"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\AzureResource\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\azuread-
vnet.virtualprivatecloud\Test_VNET.network"} -ProvisioningSchemeName
"AzureADJoinedCatalog" -RunAsynchronously -Scope @() -SecurityGroup @()
-ServiceOffering "XDHyp:
\HostingUnits\AzureResource\serviceoffering.folder\Standard_DS1_v2.service
offering"
```

To create a Microsoft Entra catalog using a prepared image. For Example:

```
New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid> -IdentityPoolUid
<IdentityPoolUid> [-CleanOnBoot] -NetworkMapping @{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.folder
\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<sunNetN
ame>.network"} -ServiceOffering <serviceofferingPath> [-MachineProfile
<machineProfilePath>] [-CustomProperties <>]
```

View the status of the Microsoft Entra join process

In Studio, the status of the Microsoft Entra join process is visible when Microsoft Entra joined machines in a delivery group are in a powered-on state. To view the status, use Search to identify those machines and then for each check **Machine Identity** on the **Details** tab in the lower pane. The following information can appear in **Machine Identity**:

- Microsoft Entra joined
- Not yet joined to Microsoft Entra ID

NOTE:

If the machines fail to be in Microsoft Entra joined state, they do not register with the Delivery Controller. Their registration status appears as **Initialization.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Also, using Studio, you can learn why machines are unavailable. To do that, click a machine on the **Search** node, check **Registration** on the **Details** tab in the lower pane, and then read the tooltip for additional information.

Delivery Group

See Create delivery groups section for details.

Enable Rendezvous

Once the delivery group has been created, you can enable Rendezvous. See Rendezvous V2 for details.

Troubleshoot

If machines fail to be Microsoft Entra joined, do the following:

- Check if the system assigned managed identity is enabled for the machines. MCS-provisioned machines must have this enabled automatically. The Microsoft Entra join process fails without a system-assigned managed identity. If the system assigned managed identity is not enabled for MCS-provisioned machines, then the possible reason is:
  - `IdentityType` of the identity pool associated with the provisioning scheme is not set to `AzureAD`. You can verify this by running `Get-AcctIdentityPool`.
- For catalogs that use master images with VDA version 2206 or earlier, check the provisioning status of the **AADLoginForWindows** extension for the machines. If the **AADLoginForWindows** extension does not exist, possible reasons are:
  - `IdentityType` of the identity pool associated with the provisioning scheme is not set to `AzureAD`. You can verify this by running `Get-AcctIdentityPool`.
  - The **AADLoginForWindows** extension installation is blocked by Azure policy.
- To troubleshoot **AADLoginForWindows** extension provisioning failures, you can check logs under `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` on the MCS-provisioned machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

MCS does not rely on the `AADLoginForWindows` extension to join a VM to Microsoft Entra ID when using a master image with VDA version 2209 or later. In this case, the `AADLoginForWindows` extension will not be installed on the MCS-provisioned machine. Therefore, `AADLoginForWindows` extension provisioning logs can't be collected.

- Check the Microsoft Entra join status and debug logs by running `dsregcmd /status` command on the MCS-provisioned machine.
- Check Windows event logs under **Application and Services Logs > Microsoft > Windows > User Device Registration**.
- Check if Microsoft Entra device management is correctly configured by running `Get-Item -LiteralPath XDHyp:\Connections\${HostingConnectionName}`.

  Ensure that the value of:

  - `AzureAdDeviceManagement` property in `CustomProperties` is **true**
  - `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` property in metadata is **true**

  If `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` is **false**, it indicates that the `ServicePrincipal` of the application used by the hosting connection is not granted with sufficient permissions to perform Microsoft Entra device management. To resolve this, assign the `ServicePrincipal` with the **Cloud Device Administrator** role.

Microsoft Entra dynamic security groups

Dynamic group rules place the VMs in the catalog to a dynamic security group based on the naming scheme of the machine catalog.

If the naming scheme of the machine catalog is Test### (where, # means number), Citrix® creates the dynamic membership rule \^*Test{3}$* in the dynamic security group. Now, if the name of the VM created by Citrix is anything from Test001 to Test999, then the VM is included in the dynamic security group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If the name of the VM created by you manually is anything from Test001 to Test999, then also the VM is included in the dynamic security group. This is one of the limitations of the dynamic security group.

The dynamic security group feature is useful when you want to manage the VMs by Microsoft Entra ID. This is also useful when you want to apply Conditional Access policies or distribute apps from Intune by filtering the VMs with Microsoft Entra dynamic security group.

You can use **PowerShell** commands to:

- Create a machine catalog with Microsoft Entra dynamic security group
- Enable security group feature for a Microsoft Entra catalog
- Delete a machine catalog with Microsoft Entra joined device security group

IMPORTANT:

- To create a machine catalog with Microsoft Entra dynamic security group, add machines to the catalog, and delete the machine catalog, you must have a Microsoft Entra access token. For information on getting the Microsoft Entra access token, see `<https://docs.microsoft.com/en-us/graph/graph-explorer/graph-explorer-features#consent-to-permissions/>`.
- To request an access token in Microsoft Entra ID, Citrix requests the **Group.ReadWrite.All** permission for the Microsoft Graph API. An Microsoft Entra user who has tenant-wide admin consent permission can grant **Group.ReadWrite.All** permission for the Microsoft Graph API. For information on how to grant tenant-wide admin consent to an application in Microsoft Entra ID, see the Microsoft document `<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent>`.
- You don't need a Microsoft Entra access token if you use a Microsoft Entra service account. For information on service accounts, see Service accounts for machine identity management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a machine catalog with Microsoft Entra dynamic security group

1. In the machine catalog setup the user interface of the web-based console, on the **Machine Identities** page, select **Microsoft Entra joined**.
2. Log in to Microsoft Entra ID.
3. Get the access token to the MS Graph API. Use this access token as a value of `$AzureADAccessToken` parameter when you run the **PowerShell** commands. You don't need a Microsoft Entra access token if you use a Microsoft Entra service account.
4. Run the following command to verify if the dynamic security group name exists in the tenant.

   ```
   Get-AcctAzureADSecurityGroup

   –AccessToken  $AzureADAccessToken

   –Name "SecurityGroupName"
   ```

   Or, run the following if you are using a Microsoft Entra service account:

   ```
   Get-AcctAzureADSecurityGroup -ServiceAccountUid <service account uid> –
   Name "SecurityGroupName"
   ```

5. Create a machine catalog using the Tenant ID, access token, and dynamic security group. Run the following command to create an IdentityPool with `IdentityType=AzureAD` and create a dynamic security group in Azure.

   ```
   New-AcctIdentityPool

   -AllowUnicode

   -IdentityPoolName "SecurityGroupCatalog"

   -NamingScheme "SG-VM-###"

   -NamingSchemeType "Numeric" -Scope @()

   -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"

   -WorkgroupMachine

   -IdentityType "AzureAD"
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-DeviceManagementType "None"

-AzureADTenantId  620387bb-9167-4bdd-8435-e3dccc58369e

-AzureADSecurityGroupName "SecurityGroupName"

-AzureADAccessToken $AzureADAccessToken
```

Or, run the following if you are using a Microsoft Entra service account:

```
New-AcctIdentityPool  -AllowUnicode -AzureADSecurityGroupName
"<security group name>" -AzureADTenantId "<Azure tenant id>"
-DeviceManagementType "Intune" -IdentityPoolName "dynamic security
group test" -IdentityType "AzureAD"  -NamingScheme "<naming scheme>"
-NamingSchemeType "Numeric" -Scope @() -ServiceAccountUid @("<service
account uid>") -StartCount 1 -WorkgroupMachine -ZoneUid "<Zone UID>"
```

Enable security group feature for a Microsoft Entra catalog

You can enable the dynamic security feature for a Microsoft Entra catalog that was created without the dynamic security group feature enabled. To do this:

1. Manually create a new dynamic security group. You can also reuse an existing dynamic security group.
2. Log in to Microsoft Entra ID, and get the access token to the MS Graph API. Use this access token as a value of `$AzureADAccessToken` parameter when you run the **PowerShell** commands.

   NOTE:

   - For information on the permissions required by the Microsoft Entra user, see `<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?pivots=portal#prerequisites/>`.
   - You don’t need a Microsoft Entra access token if you use a Microsoft Entra service account.

3. Run the following command to connect the identity pool to the created Microsoft Entra dynamic security group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-AcctIdentityPool

-IdentityPoolName "SecurityGroupCatalog"

-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e

-AzureADSecurityGroupNam "ExistingSecurityGroupName"

-AzureADAccessToken $AzureADAccessToken
```

Or, run the following if you are using a Microsoft Entra service account:

```
Set-AcctIdentityPool

-IdentityPoolName "SecurityGroupCatalog"

-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e

-AzureADSecurityGroupNam "ExistingSecurityGroupName"

-ServiceAccountUid @("<service account uid>") -StartCount 1
-WorkgroupMachine -ZoneUid "<Zone UID>"
```

If you update the naming scheme, Citrix updates the naming scheme to a new membership rule. If you delete the catalog, the membership rule gets deleted, and not the security group.

Delete a machine catalog with Microsoft Entra joined device security group

When you delete a machine catalog, the Microsoft Entra joined device security group is also deleted.

To delete the Microsoft Entra dynamic security group, do the following:

1. Log in to Microsoft Entra ID.
2. Get the access token to the MS Graph API. Use this access token as value of `$AzureADAccessToken` parameter when you run the **PowerShell** commands. You don't need a Microsoft Entra access token if you use a Microsoft Entra service account.
3. Run the following command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Remove-AcctIdentityPool

-IdentityPoolName "SecurityGroupCatalog"

-AzureADAccessToken $AzureADAccessToken
```

Or, run the following if you are using a Microsoft Entra service account:

```
Remove-AcctIdentityPool

-IdentityPoolName "SecurityGroupCatalog"

-ServiceAccountUid @("<service account uid>") -StartCount 1
-WorkgroupMachine -ZoneUid "<Zone UID>"
```

Create a Microsoft Entra dynamic security group under an existing Microsoft Entra ID assigned security group

You can create a Microsoft Entra dynamic security group under an existing Microsoft Entra ID assigned security group. You can do the following:

- Get security group information.
- Get all Microsoft Entra ID assigned security groups that are synced from on-premises AD server or the assigned security groups to which Microsoft Entra roles can be assigned.
- Get all Microsoft Entra dynamic security groups.
- Add the Microsoft Entra dynamic security group as a member of the Microsoft Entra ID assigned group.
- Remove the membership between Microsoft Entra dynamic security group and Microsoft Entra ID assigned security group when Microsoft Entra dynamic security group is deleted along with the machine catalog.

You can also see explicit error messages when any of the operations fail.

Requirement:

You must have the access token to the MS Graph API when you run the **PowerShell** commands. You don't need a Microsoft Entra access token if you use a Microsoft Entra service account. Therefore, instead of `-AccessToken <token>`, use ServiceAccountUid `<service account uid>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To get the access token:

1. Open Microsoft graph explorer and log in to Microsoft Entra ID.
2. Make sure that you have consent to **Group.ReadWrite.All** and **GroupMember.ReadWrite.All** permissions.
3. Get access token from Microsoft graph explorer. Use this access token when you run the **PowerShell** commands.

To get security group information by group id:

1. Get the access token.
2. Find group object id from the Azure portal.
3. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup

-AccessToken <token> -GroupId <GroupUid>
```

Or, run the following if you are using a Microsoft Entra service account:

```
Get-AcctAzureADSecurityGroup -ServiceAccountUid <guid> -GroupId
<GroupUid>
```

To get security groups by group display the name:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup

-AccessToken <token>

-Name <TargetGroupDisplayName>
```

Or, run the following if you are using a Microsoft Entra service account:

```
Get-AcctAzureADSecurityGroup

-ServiceAccountUid <guid>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-Name <TargetGroupDisplayName>
```

To get security groups whose display the name contains a substring:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup

-AccessToken <token>

-SearchString <displayNameSubString>
```

Or, run the following if you are using a Microsoft Entra service account:

```
Get-AcctAzureADSecurityGroup

-ServiceAccountUid <guid>

-SearchString <displayNameSubString>
```

To get all Microsoft Entra ID assigned security groups that are synced from on-premises AD server or the assigned security groups to which Microsoft Entra roles can be assigned:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup

-AccessToken <token>

-Assigned true
```

Or, run the following if you are using a Microsoft Entra service account:

```
Get-AcctAzureADSecurityGroup

-ServiceAccountUid <guid>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-Assigned true
```

To get all Microsoft Entra dynamic security groups:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup

-AccessToken <token>

-Dynamic true
```

Or, run the following if you are using a Microsoft Entra service account:

```
Get-AcctAzureADSecurityGroup

-ServiceAccountUid <guid>

-Dynamic true
```

To get Microsoft Entra ID assigned security groups with maximum record count:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroup

-AccessToken <token>

-Assigned true

-MaxRecordCount 10
```

Or, run the following if you are using a Microsoft Entra service account:

```
Get-AcctAzureADSecurityGroup

-ServiceAccountUid <guid>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-Assigned true

-MaxRecordCount 10
```

To add Microsoft Entra dynamic security group as a member of Microsoft Entra ID assigned security group:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Add-AcctAzureADSecurityGroupMember

-AccessToken <token>

-GroupId <ASG-Id>

-RefGroupId <DSG-Id>
```

Or, run the following if you are using a Microsoft Entra service account:

```
Add-AcctAzureADSecurityGroupMember

-ServiceAccountUid <guid>

-GroupId <ASG-Id>

-RefGroupId <DSG-Id>
```

To get Microsoft Entra ID assigned security group members:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Get-AcctAzureADSecurityGroupMember

-AccessToken <token>

-GroupId <ASG-Id>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Or, run the following if you are using a Microsoft Entra service account:

```
Get-AcctAzureADSecurityGroupMember

-ServiceAccountUid <guid>

-GroupId <ASG-Id>
```

NOTE:

`Get-AcctAzureADSecurityGroupMember` provides you only the direct members of the security group type under Microsoft Entra ID assigned security group.

To remove the membership between Microsoft Entra dynamic security group and Microsoft Entra ID assigned security group when Microsoft Entra dynamic security group is deleted along with machine catalog:

1. Get the access token.
2. Run the following **PowerShell** command in the **PowerShell** console:

```
Remove-AcctIdentityPool

-IdentityPoolName "SecurityGroupCatalog"

-AzureADAccessToken $AzureADAccessToken
```

Or, run the following if you are using a Microsoft Entra service account:

```
Remove-AcctIdentityPool

-ServiceAccountUid <guid>

-IdentityPoolName "SecurityGroupCatalog"
```

Modify Microsoft Entra dynamic security group name

You can modify the Microsoft Entra dynamic security group name associated with a machine catalog. This modification makes the security group information stored in the Microsoft Entra identity pool object to be consistent with the information stored in the Azure portal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The Microsoft Entra dynamic security groups do not include security groups synced from on-premises AD and other group types like Office 365 group.

You can modify the Microsoft Entra dynamic security group name using Studio and PowerShell commands.

To modify the Microsoft Entra dynamic security group name using **PowerShell**:

1. Open the **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific **PowerShell** modules.
3. Run the command `Set-AcctIdentityPool -AzureAdSeurityGroupName [DSG-Name]`.

You get appropriate error messages if the Microsoft Entra dynamic security group name cannot be modified.

More information

- Service accounts for machine identity management
- Microsoft Entra service accounts

Identity pool of Microsoft Entra hybrid joined machine identity

This article describes how to create identity pool of Microsoft Entra hybrid joined machine identity using Citrix DaaS.

For information on requirements, limitations, and considerations, see Microsoft Entra hybrid joined.

Use Studio

The following information is a supplement to the guidance in Create machine catalogs. To create Microsoft Entra hybrid joined catalogs, follow the general guidance in that article, minding the details specific to Microsoft Entra hybrid joined catalogs.

In the catalog creation wizard:

1. On the **Machine Identities** page:
    a. Select the identity type as **Microsoft Entra hybrid joined**.
    b. Under Advanced configurations, click **Select service account** and select an available service account from the list. If a suitable service account is not available that the machine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

identities will join to, you can create a service account. For information on service account, see Microsoft Entra service accounts.

c. Click **Add Extension Attributes** to store unique, custom data directly on your Entra ID device objects. On the **Add Extension Attributes** page, add **Extension attributes** and **Value**.

> **NOTE:**
>
> - You can add a maximum of 15 extension attributes.
> - The name and value must be unique and can't be empty.

d. Select an Active Directory account option:

- **Create new Active Directory accounts**:
  - If you select **Create new Active Directory accounts** and do use an existing identity pool to create new accounts, then select a domain for those accounts and specify an account naming scheme.
  - If you select **Create new Active Directory accounts** and use an existing identity pool to create new accounts, then select an identity pool from the list.
- **Use existing Active Directory accounts**: You can browse or import from a CSV file, and reset the password or specify the same password for all accounts.

e. Click **Next**.

2. On the **Domain credentials** page, select a service account or enter credentials manually. Microsoft Entra hybrid joined identity pool can also be associated with an on-premises AD service account. For information on service accounts, see On-premises Active Directory service accounts.

Add or modify extension attributes

To change or add additional extension attributes to an existing MCS machine catalog, or add extension attributes to an MCS catalog without a service account, use the **Edit Machine Catalog** wizard.

- To change or add additional extension attributes, navigate to the **Microsoft Entra Device Extension Attributes** page. Click the pencil icon, and add or update extension attributes.
- To add extension attributes to an MCS catalog without a Microsoft Entra service account:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Navigate to the **Service Account** page. Select a Microsoft Entra service account for the Microsoft Intra ID.

b. Go to the Microsoft Entra Device Extension Attributes page, click **Add Extension Attributes**.

Use PowerShell

The following PowerShell steps are equivalent to operations in Studio.

The difference between on-premises AD joined catalogs and Microsoft Entra hybrid joined ones lies in the creation of the identity pool and the machine accounts.

Create new identity pool

For example: To create an identity pool along with the accounts for Microsoft Entra hybrid joined catalogs:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

NOTE:

The `$password` is the matching password for an AD user account with Write Permissions.

All other commands used to create Microsoft Entra hybrid joined catalogs are the same as for traditional on-premises AD joined catalogs.

You can also associate an on-premises service account with an MCS created machine catalog by associating an on-premises service account with the identity pool. You can create an identity pool or update an existing identity pool to associate it with a service account.

For example: To create a new identity pool and associate it with a service account, run the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05" -ServiceAccountUid $serviceAccountUid
```

For example: To create a new identity pool with specified extension attributes and associate it with a service account, run the following:

```
New-AcctIdentityPool -IdentityPoolName HybridAzureAD -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType HybridAzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

When a VM is powered on for the first time, after joining Microsoft Entra ID, the VM reports its Entra ID deviceId to MCS.

For example: To check the `EntraIDDeviceID`, run `Get-AcctADAccount` or `Get-AcctIdentity`.

```
Get-AcctADAccount -IdentityPoolName MyPool
```

After reboot, for persistent and non-persistent VMs, the `EntraIDDeviceID` remains the same.

NOTE:

MCS automatically removes associated device IDs and extension attributes when you delete a VM from the catalog but don't delete from Azure.

Update existing identity pool

For example: To update an existing identity pool to associate it with a service account, run the following:

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

NOTE:

The `$serviceAccountUid` must be a valid UID of an on-premises Active Directory service account.

For example: To edit extension attributes for the existing catalog, run the following:

NOTE:

- After upgrading existing catalog VMs to VDA version 2511 or later, a reboot is necessary. This reboot allows the VM to report its Entra ID deviceId to MCS, enabling MCS to then configure the VM's extension attributes.
- The existing catalog should have an AzureAD type of service account with permission "Device.ReadWrite.All".

To add some new attributes:

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

To remove some existing attributes

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

OR

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` also updates the Entra ID device's extension attributes for VMs that are already joined to Entra ID and possess an `EntraIDDeviceID` value within their identities.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a Hybrid Microsoft Entra catalog

You can also create a Hybrid Microsoft Entra catalog using a prepared image. For the complete set of PowerShell commands to create image definition, image version, and prepared image version spec, see:

- Azure virtualization environment: Use PowerShell.
- VMware virtualization environment: Use PowerShell

After creating the prepared image version spec, create the identity pool and machine catalog. For example:

```
New-AcctIdentityPool -IdentityPoolName "mypool" -NamingScheme ACC##  -
NamingSchemeType "Numeric"  -ZoneUid $zoneuid -Domain $domainName -OU
"OU=HAAD Computers,DC=haad,DC=link" -IdentityType "HybridAzureAD"



New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid> -IdentityPoolUid
<IdentityPoolUid> [-CleanOnBoot] -NetworkMapping @{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.folder
\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<sunNetN
ame>.network"} -ServiceOffering <serviceofferingPath> [-MachineProfile
<machineProfilePath>] [-CustomProperties <>]
```

View the status of the hybrid Microsoft Entra join process

In Studio, the status of the hybrid Microsoft Entra join process is visible when Microsoft Entra hybrid joined machines in a delivery group are in a powered-on state. To view the status, use Search to identify those machines and then for each check **Machine Identity** on the **Details** tab in the lower pane. The following information can appear in **Machine Identity**:

- Microsoft Entra hybrid joined
- Not yet joined to Microsoft Entra ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- You might experience delayed hybrid Microsoft Entra join when the machine initially powers on. This is caused by the default machine identity sync interval (30 minutes of Microsoft Entra Connect). The machine is in Microsoft Entra hybrid joined state only after the machine identities are synced to Microsoft Entra ID through Microsoft Entra Connect.
- If machines fail to be in Microsoft Entra hybrid joined state, they are not registered with the Delivery Controller. Their registration status appears as **Initialization**.

Also, using Studio, you can learn why machines are unavailable. To do that, click a machine on the **Search** node, check **Registration** on the **Details** tab in the lower pane, and then read the tooltip for additional information.

Troubleshoot

If machines fail to be Microsoft Entra hybrid joined, do the following:

- Check if the machine account has been synced to Microsoft Entra ID through the Microsoft Microsoft Entra portal. If synced, **Not yet joined to Microsoft Entra ID** appears, indicating pending registration status.

  To sync machine accounts to Microsoft Entra ID, make sure:

  - The machine account is in the OU that is configured to be synced with Microsoft Entra ID. Machine accounts without the **userCertificate** attribute are not synced to Microsoft Entra ID even they are in the OU that is configured to be synced.
  - The attribute **userCertificate** populates in the machine account. Use Active Directory Explorer to view the attribute.
  - Microsoft Entra Connect must have been synced at least once after the machine account is created. If not, manually run the `Start-ADSyncSyncCycle -PolicyType Delta` command in the PowerShell console of the Microsoft Entra Connect machine to trigger an immediate sync.

- Check if the Citrix managed device key pair for hybrid Microsoft Entra join is correctly pushed to the machine by querying the value of **DeviceKeyPairRestored** under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**.

  Verify that the value is 1. If not, then possible reasons are:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - `IdentityType` of the identity pool associated with the provisioning scheme is not set to `HybridAzureAD`. You can verify this by running `Get-AcctIdentityPool`.
  - The machine is not provisioned using the same provisioning scheme of the machine catalog.
  - The machine is not joined to the local domain. Local domain joined is a prerequisite of the hybrid Microsoft Entra join.

- Check diagnostic messages by running the `dsregcmd /status /debug` command on the MCS-provisioned machine.
  - If hybrid Microsoft Entra join is successful, **AzureAdJoined** and **DomainJoined** are **YES** in the output of the command line.
  - If not, refer to the Microsoft documentation to troubleshoot the issues: `<https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`.
  - If you get the error message **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**, then run the following PowerShell command to repair the user certificate:

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
    UserCertificate
    ```

For more information about the user certificate issue, see CTX566696.

Identity pool of Microsoft Intune enabled machine identity

This article describes how to create identity pool of Microsoft Intune enabled machine identity using Citrix DaaS.

You can create:

- Microsoft Entra joined catalogs enrolled in Microsoft Intune for persistent and non-persistent, single and multi-session VMs. For creating catalogs, see Create Microsoft Entra catalogs enrolled in Microsoft Intune.
- Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune for persistent single and multi-session VMs using device credential with co-management capability. For creating catalogs, see Create Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune. You can also create Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune for non-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

persistent single and multi-session VMs. However, this is currently under Preview. See Enrollment of Hybrid Entra ID joined non-persistent VMs into Microsoft Intune.

For information on requirements, limitations, and considerations, see Microsoft Intune.

Create Microsoft Entra catalogs enrolled in Microsoft Intune

You can create Microsoft Entra catalogs enrolled in Microsoft Intune for persistent and non-persistent VMs using both Studio and PowerShell.

For information on requirements, limitations, and considerations, see:

- Requirements for Microsoft Entra joined catalogs enrolled in Microsoft Intune
- Limitations for Microsoft Entra joined catalogs enrolled in Microsoft Intune

Use Studio

The following information is a supplement to the guidance in Create machine catalogs.

In the catalog creation wizard:

- On the **Machine Identities** page:
  - Select **Microsoft Entra joined** and then **Enroll the machines in Microsoft Intune**. If enabled, enroll the machines in Microsoft Intune for management. You can create Microsoft Entra joined catalogs enrolled in Microsoft Intune for both persistent and non-persistent single-session and multi-session VMs. However, for non-persistent VMs, you must have the VDA version as 2407 or later.
  - Click **Select service account** and select an available service account from the list. If a suitable service account is not available for the Microsoft Entra tenant that the machine identities will join to, you can create a service account. For information on service account, see Microsoft Entra service accounts.

    NOTE:

    The service account that you selected might be in an unhealthy status due to various reasons. You can go to **Administrators > Service Accounts** to view details and fix the issues according to the recommendations. Alternatively, you can proceed with the machine catalog operation and fix the issues later. If you do not fix the issue, stale Microsoft Entra joined or Microsoft Intune enrolled devices are generated that can block Microsoft Entra join of the machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Click **Add Extension Attributes** to store unique, custom data directly on your Entra ID device objects. On the **Add Extension Attributes** page, add **Extension attributes** and **Value**.

  NOTE:

  - You can add a maximum of 15 extension attributes.
  - The name and value must be unique and can’t be empty.

Add or modify extension attributes

To change or add additional extension attributes to an existing MCS machine catalog, or add extension attributes to an MCS catalog without a service account, use the **Edit Machine Catalog** wizard.

- To change or add additional extension attributes, navigate to the **Microsoft Entra Device Extension Attributes** page. Click the pencil icon, and add or update extension attributes.
- To add extension attributes to an MCS catalog without a Microsoft Entra service account:

  a. Navigate to the **Service Account** page. Select a Microsoft Entra service account for the Microsoft Intra ID.

  b. Go to the Microsoft Entra Device Extension Attributes page, click **Add Extension Attributes**.

Use PowerShell

The following are the PowerShell steps that are equivalent to operations in Studio.

To enroll machines in Microsoft Intune using the Remote PowerShell SDK, use the `DeviceManagementType` parameter in `New-AcctIdentityPool`. This feature requires that the catalog is Microsoft Entra joined and that Microsoft Entra ID possesses the correct Microsoft Intune license. For example:

```
New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"
IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName
"AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -NamingSchemeType
"Numeric" -ServiceAccountUid $serviceAccountUid -Scope @() -ZoneUid
"81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example: To create a new identity pool with specified extension attributes and associate it with a service account, run the following:

```
New-AcctIdentityPool -IdentityPoolName MyPool -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType AzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

When a VM is powered on for the first time, after joining Microsoft Entra ID, the VM reports its Entra ID deviceId to MCS.

For example: To check the `EntraIDDeviceID`, run `Get-AcctADAccount` or `Get-AcctIdentity`.

```
Get-AcctADAccount -IdentityPoolName MyPool
```

After reboot, for persistent VMs, the `EntraIDDeviceID` remains the same. For non-persistent VMs, there is a new `EntraIDDeviceID` after every reboot.

NOTE:

MCS automatically removes associated extension attributes when you delete a VM from the catalog but don’t delete from Azure.

For example: To edit extension attributes for the existing catalog, run the following:

NOTE:

- After upgrading existing catalog VMs to VDA version 2511 or later, a reboot is necessary. This reboot allows the VM to report its Entra ID deviceId to MCS, enabling MCS to then configure the VM's extension attributes.
- The existing catalog should have an AzureAD type of service account with permission "Device.ReadWrite.All".

To add some new attributes:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

To remove some existing attributes

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

OR

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` also updates the Entra ID device's extension attributes for VMs that are already joined to Entra ID and possess an `EntraIDDeviceID` value within their identities.

For example: To create a Microsoft Entra catalog enrolled in Microsoft Intune using a prepared image:

```
New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid> -IdentityPoolUid
<IdentityPoolUid> [-CleanOnBoot] -NetworkMapping @{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.folder
\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<sunNetN
ame>.network"} -ServiceOffering <serviceofferingPath> [-MachineProfile
<machineProfilePath>] [-CustomProperties <>]
```

Troubleshoot

If machines fail to enroll in Microsoft Intune, do the following:

- Check if the MCS-provisioned machines are Microsoft Entra joined. The machines fail to enroll in Microsoft Intune if they are not Microsoft Entra joined. See Troubleshoot to troubleshoot Microsoft Entra join issues.
- Check if your Microsoft Entra tenant is assigned with the appropriate Intune license. See `<https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses>` for license requirements of Microsoft Intune.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For catalogs that use master images with VDA version 2206 or earlier, check the provisioning status of the **AADLoginForWindows** extension for the machines. If the **AADLoginForWindows** extension does not exist, possible reasons are:
  - `IdentityType` of the identity pool associated with the provisioning scheme is not set to `AzureAD` or `DeviceManagementType` is not set to `Intune`. You can verify this by running `Get-AcctIdentityPool`.
  - Azure policy has blocked the **AADLoginForWindows** extension installation.
- To troubleshoot **AADLoginForWindows** extension provisioning failures, you can check logs under `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` on the MCS provisioned machine.

  NOTE:

  MCS does not rely on the `AADLoginForWindows` extension to join a VM to Microsoft Entra ID and enroll to Microsoft Intune when using a master image with VDA version 2209 or later. In this case, the `AADLoginForWindows` extension is not installed on the MCS-provisioned machine. Therefore, `AADLoginForWindows` extension provisioning logs can't be collected.

- Check Windows event logs under **Application and Services Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider**.
- The service account that you selected might be in an unhealthy status due to various reasons. You can go to **Administrators > Service Accounts** to view details and fix the issues according to the recommendations. If you do not fix the issue, stale Microsoft Entra joined or Microsoft Intune enrolled devices are generated that can block Microsoft Entra join of the machines.

Create Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune

You can create co-management enabled catalogs for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune for persistent single and multi-session VMs. You can create co-management enabled catalogs using both Studio and PowerShell.

For information on requirements, limitations, and considerations, see:

- Requirements for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune
- Limitations for Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use Studio

The following information is a supplement to the guidance in Create machine catalogs.

In the **Machine Catalog Setup** wizard:

- On the **Machine Identities** page, select **Microsoft Entra hybrid joined** and then **Enroll the machines in Microsoft Intune with Configuration Manager**. Using this action, Configuration Manager and Microsoft Intune (that is, co-managed) manages the VMs.
- Click **Add Extension Attributes** to store unique, custom data directly on your Entra ID device objects. On the **Add Extension Attributes** page, add **Extension attributes** and **Value**.

  NOTE:

  - You can add a maximum of 15 extension attributes.
  - The name and value must be unique and can’t be empty.

Add or modify extension attributes

To change or add additional extension attributes to an existing MCS machine catalog, or add extension attributes to an MCS catalog without a service account, use the **Edit Machine Catalog** wizard.

- To change or add additional extension attributes, navigate to the **Microsoft Entra Device Extension Attributes** page. Click the pencil icon, and add or update extension attributes.
- To add extension attributes to an MCS catalog without a Microsoft Entra service account:

  a. Navigate to the **Service Account** page. Select a Microsoft Entra service account for the Microsoft Intra ID.

  b. Go to the Microsoft Entra Device Extension Attributes page, click **Add Extension Attributes**.

Use PowerShell

The following are the PowerShell steps equivalent to steps in Studio.

To enroll machines in Microsoft Intune with Configuration Manager using the Remote PowerShell SDK, use the `DeviceManagementType` parameter in `New-AcctIdentityPool`. This feature requires that the catalog is Microsoft Entra hybrid joined and that Microsoft Entra ID possesses the correct Microsoft Intune license.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The difference between Microsoft Entra hybrid joined catalogs and co-management enabled ones lies in the creation of the identity pool. For example:

```
New-AcctIdentityPool -AllowUnicode -DeviceManagementType "IntuneWithSCCM"
IdentityType="HybridAzureAD" -IdentityPoolName "CoManagedCatalog"
-NamingScheme "CoManaged-VM-##" -NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

For example: To create a new identity pool with specified extension attributes and associate it with a service account, run the following:

```
New-AcctIdentityPool -IdentityPoolName HybridAzureAD -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType HybridAzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

When a VM is powered on for the first time, after joining Microsoft Entra ID, the VM reports its Entra ID deviceId to MCS.

For example: To check the `EntraIDDeviceID`, run `Get-AcctADAccount` or `Get-AcctIdentity`.

```
Get-AcctADAccount -IdentityPoolName MyPool
```

After reboot, for persistent and non-persistent VMs, the `EntraIDDeviceID` remains the same.

NOTE:

MCS automatically removes associated device IDs and extension attributes when you delete a VM from the catalog but don’t delete from Azure.

For example: To edit extension attributes for the existing catalog, run the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- After upgrading existing catalog VMs to VDA version 2511 or later, a reboot is necessary. This reboot allows the VM to report its Entra ID deviceId to MCS, enabling MCS to then configure the VM's extension attributes.
- The existing catalog should have an AzureAD type of service account with permission "Device.ReadWrite.All".

To add some new attributes:

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

To remove some existing attributes

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

OR

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` also updates the Entra ID device's extension attributes for VMs that are already joined to Entra ID and possess an `EntraIDDeviceID` value within their identities.

You can also create a persistent Hybrid Microsoft Entra catalog enrolled in Microsoft Intune using a prepared image. For the complete set of PowerShell commands to create image definition, image version, and prepared image version spec, see:

- Azure virtualization environment: Use PowerShell.
- VMware virtualization environment: Use PowerShell

After creating the prepared image version spec, create the identity pool and machine catalog. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-AcctIdentityPool -IdentityPoolName "mypool" -NamingScheme ACC##  -
NamingSchemeType "Numeric"  -ZoneUid $zoneuid -Domain $domainName -OU
"OU=HAAD Computers,DC=haad,DC=link" -IdentityType "HybridAzureAD"
-DeviceManagement IntuneWithSCCM



New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid> -IdentityPoolUid
<IdentityPoolUid> [-CleanOnBoot] -NetworkMapping @{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.folder
\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<sunNetN
ame>.network"} -ServiceOffering <serviceofferingPath> [-MachineProfile
<machineProfilePath>] [-CustomProperties <>]
```

NOTE:

Enrollment of Microsoft Entra hybrid joined non-persistent VMs into Microsoft Intune is currently under preview.

Troubleshoot

If machines fail to enroll in Microsoft Intune or fail to reach co-management state, do the following:

- Check Intune license

  Check if your Microsoft Entra tenant is assigned with the appropriate Intune license. See Microsoft Intune licensing for license requirements of Microsoft Intune.

- Check Hybrid Microsoft Entra join status

  Check if the MCS-provisioned machines are Microsoft Entra hybrid joined. The machines are not eligible for co-management if not Microsoft Entra hybrid joined. See Troubleshoot to troubleshoot Hybrid Microsoft Entra join issues.

- Check co-management eligibility

  - Check if the MCS-provisioned machines are correctly assigned with the expected Configuration Manager site. To get the assigned site, run the following PowerShell command on the affected machines.

    ```
    (New-Object -ComObject "Microsoft.SMS.Client").GetAssignedSite()
    ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If no site is assigned to the VM, use the following command to check if the Configuration Manager site can be automatically discovered.

  ```
  (New-Object -ComObject "Microsoft.SMS.Client").AutoDiscoverSite()
  ```

- Ensure that boundaries and boundary groups are well configured in your Configuration Manager environment if no site code can be discovered. See Considerations for details.
- Check `C:\Windows\CCM\Logs\ClientLocation.log` for any Configuration Manager client site assignment issues.
- Check the co-management states of the machines. Open the **Configuration Manager control panel** on the affected machines and go to the **General** tab. The value of Co-management property must be **Enabled**. If not, check logs under `C:\Windows\CCM\Logs\CoManagementHandler.log`.

- Check Intune enrollment

  Machines might fail to enroll in Microsoft Intune even if all prerequisites are satisfied. Check Windows event logs under **Application and Services Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider** for Intune enrollment issues.

More information

- Service accounts for machine identity management
- Microsoft Entra service accounts

Identity pool of non-domain-joined machine identity

This article describes how to create identity pool of non-domain-joined machine identity using Citrix DaaS.

For information on requirements, limitations, and considerations, see Non-domain-joined.

Before you create the machine catalog, you need the following:

1. New resource location

   - Navigate to the Citrix Cloud™ admin UI > upper left hamburger menu > **Resource Locations**.
   - Click **+ Resource Location**.
   - Enter a name for the new resource location and click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Create a hosting connection. See Create and manage connections section for details.

Using Citrix DaaS, you can create catalogs based on workgroups for non-domain-joined machines. Creating non-domain-joined machines depends on how the account identity pool is created. The account identity pool is the mechanism used by MCS to create and track machine names during catalog provisioning.

You can create non-domain-joined catalogs by using Studio or PowerShell.

Use Studio

The following information is a supplement to the guidance in Create machine catalogs. To create non-domain-joined catalogs, follow the general guidance in that article, minding the details specific to non-domain-joined catalogs.

In the catalog creation wizard:

- On the **Machine Identities** page, select **Non-domain-joined**. The created machines are not joined to any domain.

NOTE:

The **Non-domain-joined** identity type requires version 1811 or later of the VDA as the minimum functional level for the catalog. To make it available, update the minimum functional level if necessary.

Use PowerShell

The following are PowerShell steps equivalent to operations in Studio.

You can create an identity pool for non-domain-joined catalogs using the Remote PowerShell SDK.

Use the PowerShell parameters, **WorkgroupMachine** and **IdentityType** to create an identity pool for non-domain-joined catalogs. The parameters eliminate the need to specify all AD-specific parameters including domain administrator credentials:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

All other commands used to create non-domain-joined catalogs are the same as for the traditional on-premises Active Directory joined catalogs.

Manage machine catalogs

NOTE:

This article describes how to manage catalogs using Studio and PowerShell commands. If you created the catalog using the Quick Deploy node, and continue using that node to manage the catalog, then follow Manage catalogs in Quick Deploy.

Introduction

You can add or remove machines from a machine catalog, and rename, change the description, or manage a catalog's Active Directory computer accounts.

Catalog maintenance can also include the tasks of making sure that each machine has the latest OS updates, antivirus software updates, operating system upgrades, or configuration changes.

- Catalogs containing pooled random machines created using Machine Creation Services™ (MCS) maintain machines by updating the image used in the catalog and then updating the machines. This method lets you update large numbers of user machines efficiently.
- For catalogs containing static, permanently assigned machines, you can manage the image or template that those catalogs currently use but only the machines you add to the catalogs later are created using the new image or template.
- For Remote PC Access catalogs, you manage updates to users' machines outside of Studio. Perform this task individually or collectively using third-party software distribution tools.

For information about creating and managing connections to host hypervisors and cloud services, see Create and manage connections and resources.

NOTE:

MCS does not support Windows 10 IoT Core and Windows 10 IoT Enterprise. Refer to the Microsoft site for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About persistent instances

When updating the master image for an MCS catalog containing persistent machines, any new machines added to the catalog use the updated image. Existing machines continue to use the original master image. The process of updating an image is done the same way for any other type of catalog. Consider the following:

- With persistent disk catalogs, the pre-existing machines are not updated to the new image, but any new machines added to the catalog use the new image.
- For non-persistent disk catalogs, the machine image is updated the next time only if the machine is restarted within Studio or PowerShell. If the machine is restarted from the hypervisor outside of Studio, the disk is not reset.
- For catalogs that do not persist, if you want different images for different machines, the images must reside in separate catalogs.

Manage Machine Catalogs

You can manage a machine catalog in two ways:

- Using Studio
- Using PowerShell

Use Studio

This section details how you can manage catalogs using Studio:

- View catalog details
- Add machines to a catalog
- Delete machines from a catalog
- Edit a catalog
- Rename a catalog
- Delete a catalog
- Manage Active Directory computer accounts in a catalog
- Change the master image for a catalog
- Convert MCS-provisioned catalogs from using master images to using prepared images.
- Change the functional level or undo the change
- Clone a catalog

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Organize catalogs using folders
- Upgrade VDAs
- Manage experience optimization settings for a catalog
- Retry catalog creation
- (Non-Citrix® provisioned VDAs only) Generate and manage enrollment tokens

View catalog details

1. Use the search function to locate a specific machine catalog. Refer to Search for instances for instructions.
2. From the search results, select a catalog as necessary.
3. Refer to the following table for descriptions of the catalog columns.

COLUMN	DESCRIPTION
Machine Catalog	The name and the allocation type of the catalog. Allocation types include
	• Random: Machines in the catalog are allocated to a user randomly.
	• Permanent: Machines in the catalog are allocated to a user permanently.
Machine Type	The supported session type of the machines in the catalog. Possible values include
	• OS type: Multi-session OS (Virtual); User data: Discard.
	• OS type: Multi-session OS (Virtual); User data: On local disk
	• OS type: Single-session OS (Remote PC Access)
	• OS type: Single-session OS (Virtual); User data: Discard
	• OS type: Single-session OS (Virtual); User data: On local disk

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION
Machine Count	The machine count in the catalog and the provisioning method. Possible provisioning methods include: Machine Creation Services (MCS machine), Manual, and Citrix Provisioning™ Services.
Allocated Count	The number of machines in the catalog assigned to a delivery group.
Folder	The location of the catalog within the **Machine Catalogs** tree. It displays the name of the folder that the catalog is in (including the trailing backslash), or `-` if the catalog is at the root level.
VDA Upgrade	VDA Upgrade State. Possible values include: Not configured, Scheduled, Available, and Up to date.
Image Status	The status of the image update of the catalog. Applicable only to non-persistent machine catalogs. Possible values include: Fully updated, Partially updated, Pending updates, Preparing

4. Click a tab in the bottom details pane for more information about a selected catalog.

TAB	DESCRIPTION
Details	Summarizes key machine catalog settings, such as machine type, provisioning method, service account, OS, and VDA version, enabling you to quickly view and manage your resources.
Template Properties	Available for MCS provisioned catalogs only.
	Displays detailed provisioning information for the selected catalog, including

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TAB	DESCRIPTION
	• Machine Template Properties
	• Hypervisor-Specific Details
	• Machine Profile Properties
Machines	Displays a paginated list of machine names in the selected catalog.
Delivery Groups	Available for Remote PC catalogs.
	Displays delivery groups associated with the selected catalog. It displays delivery group name and catalog association.
Tags	Not available in multi-tenant environments.
	Displays tag name and description of the tags assigned to the selected machine catalog.
Workspace Environment Management	Only visible when WEM service is provisioned and accessible.
	Displays Workspace Environment Management System optimization settings.
Cost Insights	Applicable to only Azure MCS catalogs, this displays
	• Total cost incurred over the past 30 days.
	• A comparison between the current 30-day total cost and the previous 30-day period.
	Access requires the Citrix **Cost Management > Manage > Read cost** permission (default for Cloud Administrators) to view the tab, and the `Microsoft.CostManagement/query/read` Azure permission to view cost details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TAB	DESCRIPTION
Troubleshoot	Displays catalog errors or warnings with recommended actions.

Add machines to a catalog

Before you start:

- Make sure the virtualization host (hypervisor or cloud service provider) has sufficient processors, memory, and storage to accommodate the additional machines.
- Make sure that you have enough unused Active Directory computer accounts. If you are using existing accounts, the number of machines you can add is limited by the number of accounts available.
- If you use Studio to create Active Directory computer accounts for the additional machines, you must have appropriate domain administrator permission.

TIP:

If the Citrix DaaS account used to add machines to the machine catalog has restricted AD permissions, add all Cloud Connectors you intend to use in the **Log on to..** screen.

To add machines to a catalog:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a machine catalog and then select **Add machines** in the action bar.
3. On the **Virtual Machines** page, select the number of virtual machines to add.
4. On the **Machine Identities** page, configure the settings as follows:

    - Select an identity from the list.
    - If applicable, indicate whether to create accounts or use existing ones, and the location (domain) for those accounts.

      If there are insufficient existing Active Directory accounts for the number of VMs you are adding, select the domain and location where the accounts are created.

      If you use existing Active Directory accounts, browse to the accounts or select **Import** and specify a `.csv` file containing account names. Make sure that there are enough accounts for all the machines you are adding. Studio manages these accounts. Allow that interface to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

reset the passwords for all the accounts, or specify the account password, which must be the same for all accounts.

- If this identity pool is used by other catalogs, you can't change it to a different pool using Studio. Instead, use the **Set-ProvScheme** PowerShell cmdlet. For more information, see the Citrix Virtual Apps and Desktops SDK Documentation.
- Specify an account naming scheme, using hash marks to indicate where sequential numbers or letters appear. For example, a naming scheme of PC-Sales-## (with 0-9 selected) results in computer accounts named PC-Sales-01, PC-Sales-02, PC-Sales-03, and so on.
- Optionally, you can specify what the account names start with.

  When specifying what the account names start with, be aware of the following scenario: If the starting numbers or letters are already in use, the first account created is named using the nearest unused numbers or letters thereafter.

  See Manage the sequence number of the machine name to customize the sequence number of machines, which are deployed using MCS, through PowerShell commands.

5. On the **Domain Credentials** page, select **Enter credentials** and enter user credentials with sufficient permissions to create machine accounts.

The machines are created as a background process, and can take much time when creating many machines. Machine creation continues even if you close the Studio.

Use CSV files to bulk add machines to a catalog

You can bulk add machines by using CSV files. The feature is available for all catalogs except catalogs provisioned through MCS.

To bulk add machines to a catalog, complete the following steps:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a machine catalog and then select **Add Machines** in the action bar. The **Add Machines** window appears.
3. Select **Add CSV File**. The **Add Machines in Bulk** window appears.
4. Select **Download CSV Template**.
5. Fill out the template file.
6. Drag or browse to the file to upload it.
7. Select **Validate** to perform validation checks on your import.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Select **Import** to complete the process.

Considerations when using CSV files to add machines

NOTE:

- For non-Active Directory users, you must type their names in this format: `<identity provider>:<user name>`. Example: `AzureAD:username`.
- VM names are case sensitive. When entering VM paths, make sure that you enter the VM names correctly.

When editing the CSV template file, keep the following in mind:

- The feature gives you more flexibility to bulk add machines through a CSV file. In the file, you can add only machines (for use with user auto-assignments) or add machines along with user assignments. Type your data in the following format:
  - For machine account and user name (samName) pairs:
  - Domain\ComputerName1, Domain\Username1
  - Domain\ComputerName2, Domain\Username1;Domain\Username2
  - Domain\ComputerName3, AzureAD:username
  - For machine accounts only:
  - Domain\ComputerName1
  - Domain\ComputerName2
  - For VM and user name pairs:
  - XDHyp: \Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\ComputerName1,Domai
  - XDHyp: \Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\ComputerName2,Domai
  - For VMs only:
  - XDHyp: \Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\ComputerName1
  - XDHyp: \Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\ComputerName2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example: `XDHyp:\Connections\xpace-scale\East US.region\vm.folder\wsvdaV3-2.vm`

where,

- `xpace-scale` is the ConnectionName: The name of the connection that you entered in **Hosting > Add Connections and Resources**. For more information, see Create a connection and resources.
- `East US.region` is the RegionName: The name of the region with `.region` as extension.
- `wsvdaV3-2.vm` is the VMName: The name of the virtual machine with `.vm` as extension.

- The maximum number of machines that a file can contain is 1,000. To import more than 1,000 machines, spread them across different files and then import those files one by one. We recommend that you import no more than 1,000 machines. Otherwise, catalog creation can take a long time to complete.

You can also export machines from a catalog on the same **Add Machines** page. The exported CSV of machines can then be used as a template when adding machines in bulk. To export machines:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a machine catalog and then select **Add Machines** in the action bar. The **Add Machines** window appears.
3. Select **Export to CSV file**. A CSV file containing a list of the machines is downloaded.
4. Open the CSV file to add or edit machines as needed. To add machines in bulk using the saved CSV file, see the previous section, Use CSV files to bulk add machines to a catalog.

NOTE:

- This feature is not available for Remote PC Access and MCS-provisioned catalogs.
- Export and import of machines in CSV files is only supported between catalogs of the same type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enroll machines to catalogs using the WebSocket VDA enrollment tool

The WebSocket VDA enrollment tool facilitates token-based enrollment for VDA machines. This tool helps you convert a connection to a WebSocket connection by adding the VDA to the machine catalog using the enrollment token.

NOTE:

This tool is designed to enroll VDA machines that haven't been enrolled in any machine catalog.

Follow the instructions to run the enrollment tool:

1. Log in to the VDA.
2. Locate the tool `EnrollMachine.exe`, in `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`.
3. Run the tool with the appropriate input parameters. For example, `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

The following table describes the input parameters of the enrollment tool:

PARAMETER NAME	REQUIRED	DESCRIPTION	EXAMPLE
`-websocket_token_stdin`	Yes	Reads the enrollment token.	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		Reads the enrollment token directly from the command line parameter.	`.\EnrollMachine.exe -websocket_token_string:<token>`
`-websocket_token_file:[token-file-path]`		Reads the enrollment token from the path provided.	`.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER NAME	REQUIRED	DESCRIPTION	EXAMPLE
`log:[log-file-path]`	No	Shows the Enrollment tool logs.	`.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]`
`-help`	No	Shows a brief help text.	`.\EnrollMachine.exe -help`

After successful enrollment, you will receive a success message on the tool and in the logs. Ensure to sign in to Studio to verify that the VDA machine is added to the catalog and that the status of the machine is registered.

Troubleshooting

By default, you can find the logs of the enrollment tool at:

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

If you have specified a different path for the logs, you can use `log:[log-file-path]` to retrieve your logs.

The following table lists the codes returned by the enrollment tool:

CODE	STRING	DESCRIPTION
0	Success	VDA is successfully added to the machine catalog.
-1	InvalidArgument	The input parameter in the enrollment token is invalid.
-2	BrokerAgentNotFound	The broker agent service is not found.
-3	TokenInvalid	The token entered is invalid.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE	STRING	DESCRIPTION
-4	TokenMissingRequiredClaims	The required claims for the token are missing, for example, CustomerId, or Enrollment URIs.
-5	InternalError	A general error has occurred.
-6	TimedOut	The task has timed out.
-7	FailedToDetermineMachineADJoinedStatus	The service that returns the machine AD joined status failed.
-8	ADMachineFailedToFindSid	The service that returns the AD machine Sid failed.
-9	EnrollRequestFailed	The request failed due to an HTTP error.
-10	EnrollResponseMissingRequiredFields	The enrollment tool response is missing the parameter `VirtualSiteId`.
-11	InsufficientPermission	You do not have the required permission to run the task.
-12	FailedToDetermineMachineAadJoinedStatus	The service that checks the machine AD join status throws an error.
-13	AadMachineFailedToFindDeviceId	The additional parameter `AAD device id` added by the system is empty.
-14	AadDeviceIdNotValid	The additional parameter `AAD device id` added by the system is not a valid GUID.
-15	NoValidMacAddress	Invalid MAC address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE	STRING	DESCRIPTION
-16	FailedToGetComputerHostNameForVdaInstanceName	Failed to get the computer host name to set the additional parameter `VdaInstanceName`.
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	Failed to open the VDA registry key to write the list of Delivery controllers.
-18	Failed Token reached the max count	Failed Token reached the max count.

Delete machines from a catalog

After you delete a machine from a machine catalog, users can no longer access it, so before deleting a machine, ensure that:

- User data is backed up or no longer required.
- All users are logged off. Turning on maintenance mode stops new connections from being made to a machine.
- Machines are powered off.

To delete machines from a catalog:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **View Machines** in the action bar.
3. Select one or more machines and then select **Delete** in the action bar.
4. If you are deleting persistent machines from the catalog, choose whether to delete them from the hypervisor or cloud service as well. If you choose to delete them, indicate whether to retain, disable, or delete their Active Directory accounts.

When you delete persistent machines from an Azure Resource Manager catalog, the machines and associated resource groups are deleted from Azure, even if you choose to retain them.

When you delete non-persistent machines from a catalog, they are automatically deleted from the hypervisor or cloud service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Edit a catalog

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Edit Machine Catalog** in the action bar.
3. On the **Scopes** page, change the scopes.
4. On the **NIC** page, perform the following actions:

   - To change the subnet mapping of an NIC, select a network from the **Associated Network** field.
   - To add a subnet mapping, select **Add NIC**, select a network from the **Associated Network** field, and click **Save**.

   Only those subnets present in the host associated with the catalog appear in the **Associated Network** field.

   You can only add NIC to Azure machine catalogs without machine profiles.

   NOTE:

   - For AWS machine catalogs, you cannot map the same subnet to more than one NIC.
   - For machine catalogs with machine profiles, the number of NICs on the catalog must be equal to the number of NICs on the machine profile.
   - This feature is not supported for IBM Cloud hypervisors.
   - This feature is supported only for Nutanix Prism Element in Nutanix hypervisors.

5. On the **VDA Upgrade** page, change or select the VDA version to upgrade to. For more information, see VDA upgrade.
6. You might see additional pages depending on the catalog type.

   For catalogs created using an Azure Resource Manager image, the following pages are visible. Keep in mind that the changes you make apply only to machines you add to the catalog later. Existing machines remain unchanged.

   - On the **Virtual Machines** page, change the machine size and availability zones where you want to create machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Only the machine sizes that the catalog supports are shown.
- If necessary, select **Show only machine sizes used in other machine catalogs** to filter the machine size list.
- For Azure catalogs, if **ZRS** is the Storage redundancy on the Storage and License Types page, then you get a warning suggesting to clear the zone selection and let Azure manage the VM availability zones.

- On the **Machine Profile** page, choose whether to use or change a machine profile.

NOTE:

For Azure catalogs, when you modify a machine profile that includes availability zones and choose ZRS for storage redundancy, a warning suggests you to clear the zone selection.

- (Only when the catalog is configured with a dedicated group host) On the **Dedicated host group** page, choose whether to change a host group.
- On the **Storage and License Types** page, choose whether to change the storage redundancy type (for Azure catalog), storage type, license type, and Azure Computer Gallery settings (available only when **Place prepared image in Azure Gallery** is in use).

NOTE:

If the newly selected setting doesn't support the current machine size, a warning dialog box appears, informing you that changing the setting, resets the machine size setting. If you choose to continue, a red dot appears next to the **Virtual Machines** menu, prompting you to select a new machine size.

For more information about settings available on the pages, see Create a machine catalog using an Azure Resource Manager image.

For Remote PC Access catalogs, the following pages are visible:

- On the **Power Management** page, change the power management settings and select a power management connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On the **Organizational Units** page, add or remove Active Directory OUs.

7. On the **Description** page, change the catalog description.
8. Click **Apply** to apply the changes you made and click **Save** to exit.

Rename a catalog

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Rename Machine Catalog** in the action bar.
3. Enter the new name.

Delete a catalog

Before deleting a catalog, ensure that:

- All users are logged off and no disconnected sessions are running.
- Maintenance mode is turned on for all machines in the catalog so that new connections cannot be made.
- All machines in the catalog are powered off.
- The catalog is not associated with a delivery group. In other words, the delivery group does not contain machines from the catalog.

To delete a catalog:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a catalog, select **More** in the action bar, and then select **Delete Machine Catalog**.
3. If the catalog contains persistent machines, indicate whether to delete those machines from the hypervisor or cloud service as well. If you choose to do so, choose whether to retain, disable, or delete their Active Directory computer accounts.
4. If necessary, select **Hide progress** to run the deletion in the background.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- When you delete an Azure Resource Manager catalog, the associated machines and resource groups are deleted from Azure, even if you choose to retain them.
- When you delete a catalog containing non-persistent machines, those machines are deleted from the hypervisor or cloud service.
- When the hypervisor or cloud service is unreachable during catalog deletion, both catalog and VM deletion fail. If needed, you can choose to delete the VM records only from your Citrix site database. To do so, select the machine catalog in the **Machine Catalogs** node, and then perform the deletion shown on the **Troubleshoot** tab. Keep in mind that this action leaves the VMs intact on the host.

Manage Active Directory computer accounts in a catalog

To manage Active Directory accounts in a machine catalog, you can:

- Free unused machine accounts by removing Active Directory computer accounts from single-session and multi-session catalogs. Those accounts can then be used for other machines.
- Add accounts so that when more machines are added to the catalog, the computer accounts are already in place. Do not use a forward slash (/) in an OU name.

To manage Active Directory accounts:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Manage AD accounts** in the action bar.
3. Choose whether to add or delete computer accounts. If you add accounts, specify what to do with the account passwords: either reset them all or enter a password that applies to all accounts.

   You might reset passwords if you do not know the current account passwords; you must have permission to perform a password reset. If you enter a password, the password is changed on the accounts as they are imported. If you delete an account, choose whether the account in an Active Directory is to be kept, disabled, or deleted.

You can also indicate whether Active Directory accounts are to be retained, disabled, or deleted when you remove machines from a catalog or delete a catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change the master image for a catalog

We recommend that you save copies or snapshots of images before you change the master image for a catalog. The database keeps a historical record of the images used with each machine catalog. If users encounter problems with the new image you deployed to their desktops, you can roll it back to the previous version, minimizing user downtime. Do not delete, move, or rename images. Otherwise, you cannot roll back the master image.

IMPORTANT:

When changing the master image for a persistent catalog, consider the following: only machines you add to the catalog later are created using the new image. We do not roll out the new image to existing machines in the catalog.

After a machine is updated, it restarts automatically.

Convert MCS-provisioned catalogs from using master images to using prepared images

To convert an MCS-provisioned catalog from using a master image to using a prepared image, follow these steps:

1. Click **Machine Catalogs** in the left pane and select a machine catalog that you want to convert. Right-click and select **Convert To Prepared Image**.
2. On the **Image** page, select a prepared image.
3. On the **Rollout strategy** page, select when you want to update this catalog with the selected prepared image.
4. On the **Summary** page, verify the details and click **Finish**.
5. Verify the details of the converted machine catalog in **Template Properties**.

Currently, this feature is available only for Azure and VMware virtualization environments.

Update or create an image

Before you change the master image for a catalog, prepare a new image on your host hypervisor by either updating an existing image or creating one.

1. On your hypervisor or cloud service provider, take a snapshot of the current VM and give the snapshot a meaningful name. This snapshot can be used to roll back the master image.
2. If necessary, power on the image, and log on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Install updates or make any required changes to the image.
4. If the image uses a Personal vDisk, update the inventory.
5. Power off the VM.
6. Take a snapshot of the VM, and give the snapshot a meaningful name that is recognized when you change the master image.

NOTE:

Although you can create a snapshot using the management interface, we recommend that you create a snapshot using the hypervisor management console, and then select that snapshot in Studio. This enables you to provide a meaningful name and description rather than an automatically generated name. For GPU images, you can change the image only through the XenServer XenCenter® console.

Change the master image

To roll out a new master image to all machines in a catalog:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Change Master Image** in the action bar.
3. On the **Image** page, select the host and the image you want to roll out.

   TIP:

   For an MCS-created catalog, you can annotate its image by adding a note for the image. A note can contain up to 500 characters. Each time you change the master image, a note-related entry is created whether you add a note. If you update a catalog without adding a note, the entry appears as null (-). To view note history for the image, select the catalog, click **Template Properties** in the low pane, and then click **View note history**.

4. On the **Rollout Strategy** page, choose when the machines in the machine catalog are changed with the new image: on the next shutdown or immediately.

   NOTE:

   The **Rollout Strategy** page is not available for persistent VMs because rollout is only applicable to non-persistent VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Verify the information on the **Summary** page and then select **Finish**. Each machine restarts automatically after it is updated.

   To track the progress of the update, locate the catalog in **Machine Catalogs** to view the inline progress bar and the step-by-step progress graph. For a non-persistent catalog, you can track its image update statuses through the **Image Update** column, including **Fully updated**, **Partially updated**, **Pending update**, and **Preparing image**.

   TIP:

   To show the **Image Update** column, select the **Columns to Display** icon in the action bar, select **Machine Catalog > Image Status**, and then click **Save**.

If you are updating a catalog using the PowerShell SDK, you can specify a hypervisor template (`VMTemplates`), as an alternative to an image or a snapshot of an image.

To roll out a new master image to the Azure based machine catalog:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select an Azure catalog and then select **Change Master Image** in the action bar.
3. On the **Change Master Image** page, select an image under Master image. The blade lists all the images that belong to the same region as those of Resources.

Rollout strategy

Changing the image on the next shutdown will immediately affect any machines not currently in use, that is, machines that do not have an active user session. A system that is in use receives the update when the current active session ends.

NOTE:

Rollout strategy is only applicable to non-persistent VMs.

Consider the following:

- New sessions cannot be launched until the update has completed on applicable machines.
- For single-session machines, machines are immediately updated when the machine is not in use, or when users are not logged in.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For a multi-session OS with child machines, restarts don't occur automatically. To apply the updated master image, restart the machines using Studio, PowerShell, or Workspace. Restarting from the machines or the hypervisors doesn't apply the update.

TIP:

Limit the number of machines being rebooted by using the advanced settings for a host connection. Use these settings to modify the actions taken for a given catalog; advanced settings vary depending on the hypervisor.

Roll back the master image

After you roll out an updated or new image, you can roll it back. This might be necessary if issues occur with the newly updated machines. When you roll back, machines in the catalog are rolled back to the last working image. Any new features that require the newer image are no longer available. As with the rollout, rolling back a machine includes a restart.

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select the catalog and then select **Roll Back Master Image** in the action bar.
3. Specify when to apply the earlier image to machines, as described for the rollout operation.

The rollback is applied only to machines that need to be reverted. For machines that have not been changed to the new or updated image (for example, machines with users who have not logged off), users do not receive notification messages and are not forced to log off.

To track the rollback progress, locate the catalog in **Machine Catalogs** to view the inline progress bar and the step-by-step progress graph.

You cannot roll back in certain scenarios, including the following. (The **Roll Back Master Image** option is not visible).

- You do not have permission to roll back.
- The catalog was not created using MCS.
- The catalog was created using an image of the OS disk.
- The snapshot used to create the catalog has become corrupted.
- User changes to the machines in the catalog do not persist.
- Machines in the catalog are running.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change the functional level or undo the change

Change the functional level for the machine catalog after you upgrade the VDAs on the machines to a newer version. We recommend upgrading all VDAs to the latest version to enable access to all the newest features.

Before changing the functional level for a machine catalog:

- Start the upgraded machines so that they register with Citrix DaaS. This lets the management interface determine that the machines in the catalog need upgrading.

To change the functional level for a catalog:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select the catalog. The **Details** tab in the lower pane displays version information.
3. Select **Change Functional Level**. If the management interface detects that the catalog must change the functional level, it displays a message. Follow the prompts. If one or more machines cannot be changed, a message explains why. To ensure that all machines function properly. We recommend you resolve those issues before clicking **Change**.

After the catalog upgrade completes, you can revert the machines to their previous VDA versions by selecting the catalog and then selecting **Undo Functional Level Change** in the action bar.

Clone a catalog

Before cloning a catalog, be aware of the following considerations:

- You cannot change settings associated with operating system and machine management. The cloned catalog inherits those settings from the original.

  NOTE:

  If you select an Azure catalog to clone and select a Master image, the blade lists all the images that belong to the same region as those of Resources.

- Cloning a catalog can take some time to complete. If necessary, select **Hide progress** to run the cloning in the background.
- The cloned catalog inherits the name of the original and has a suffix `Copy`. You can change the name. See Rename a catalog.
- After cloning completes, be sure to assign the cloned catalog to a delivery group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can create an empty catalog by cloning. During catalog cloning, you can set the number of machines to zero for MCS-provisioned catalogs and add no machines for non-MCS-provisioned catalogs.

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select a catalog and then select **Clone** in the action bar.
3. In the **Clone Selected Machine Catalog** window, view the settings for the cloned catalog and configure settings as applicable. Select **Next** to proceed to the next page.
4. On the **Summary** page, view a summary of the settings and select **Finish** to start cloning.
5. If necessary, select **Hide progress** to run the cloning in the background.

Organize catalogs using folders

You can create folders to organize catalogs for easy access. For example, you can organize catalogs by image type or by organization structure.

TIP:

You can set your preferred default view (folder or list view) for the Machine Catalogs node by clicking the **Folder** icon on the top right of the action bar.

Required roles

By default, you need to have the following built-in role to create and manage catalog folders: Cloud Administrator, Full Administrator, or Machine Catalog Administrator. If necessary, you can customize roles for creating and managing catalog folders. For more information, see Required permissions.

Create a catalog folder

Before you start, first plan how to organize your catalogs. Consider the following:

- You can nest folders up to five levels deep (excluding the default root folder).
- A catalog folder can contain catalogs and subfolders.
- All nodes in Studio (such as **Machine Catalogs**, **Delivery Groups**, **Applications**, and **Application Groups**) share the same folder tree in the back end. To avoid name conflicts when renaming or moving folders, use unique names for first-level folders across different nodes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you create a folder using the `New-BrokerAdminFolder` SDK cmdlet and want it to appear under the **Machine Catalogs** node, you must add the `ContainsMachineCatalogs` metadata using the `Set-BrokerAdminFolderMetadata` cmdlet.

Example:

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsMachineCatalogs -Value true
```

To create a catalog folder, follow these steps:

1. From Studio, select **Machine Catalogs** in the left pane.
2. In the folder hierarchy, select a folder and then select **Create Folder** in the **Action** bar.
3. Enter a name for the new folder, and then click **Done**.

TIP:

If you create a folder in an unintended location, you can drag it to the correct location.

Move a catalog

You can move a catalog between folders. Detailed steps are as follows:

1. From Studio, select **Machine Catalogs** in the left pane.
2. View catalogs by folder. You can also turn on **View all** above the folder hierarchy to view all catalogs at a time.
3. Right-click a catalog and then select **Move Machine Catalog**.
4. Select the folder to which you want to move the catalog, and then click **Done**.

TIP:

You can drag a catalog to a folder.

Manage catalog folders

You can delete, rename, and move catalog folders.

You can delete a folder only if it and its subfolders don't contain catalogs.

To manage a folder, follow these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. From Studio, select **Machine Catalogs** in the left pane.
2. In the folder hierarchy, select a folder, and then select an action in the **Action** bar as needed:
   - To rename the folder, select **Rename Folder**.
   - To delete the folder, select **Delete Folder**.
   - To move the folder, select **Move Folder**.
3. Follow the onscreen instructions to complete the remaining steps.

Required permissions

The following table lists the permissions required to do actions on catalog folders.

ACTION	REQUIRED PERMISSIONS
Create catalog folders	Create Machine Catalog Folder
Delete catalog folders	Remove Machine Catalog Folder
Move catalog folders	Move Machine Catalog Folder
Rename catalog folders	Edit Machine Catalog Folder
Move catalogs to folders	Edit Machine Catalog Folder and Edit Machine Catalog Properties

Upgrade VDAs

You can use the Studio interface to upgrade VDAs with ease. For more information and step-by-step guidance, see Citrix VDA Upgrade Service documentation.

Manage experience optimization settings for a catalog

Before you start, make sure that your **Workspace Environment Management (WEM)** service deployment is set up. For more information, see Get started with Workspace Environment Management service.

Required permissions

By default, creating and managing configuration sets for machine catalogs requires the **WEM Full Administrator** role, along with one of the following roles:

- **Full Access Administrator**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Cloud Administrator**
- **Machine Catalog Administrator**

To allow other roles to manage configuration sets, assign them both the **Manage configuration sets** permission and the **WEM Full Administrator** role.

Edit the experience optimization settings

Select an **Experience Optimization** option to apply to the catalog:

- **Apply default settings:** Select this option to apply the default optimization settings, including automatic CPU spike protection and intelligent CPU optimization.
- **Apply custom settings:** Enter a name to create a configuration set, then customize the optimization settings according to your requirements. Alternatively, you can select an existing configuration set.

Retry catalog creation

NOTE:

This feature applies only to MCS catalogs.

Failed catalogs are marked with an error icon. To see the details, go to the **Troubleshoot** tab of each catalog. Before retrying catalog creation, be aware of the following considerations:

- Check the troubleshooting information first and resolve the issues. The information describes the issues found and provides recommendations for resolving them.
- You cannot change settings associated with Operating system and machine management. The catalog inherits those settings from the original.
- The creation can take some time to complete. If necessary, select **Hide progress** to run the creation in the background.

To retry creating a catalog, do the following:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select the catalog and then go to its **Troubleshoot** tab.
3. Click the retry hyperlink to retry creating the catalog.
4. In the wizard that appears, change settings where necessary. If there is no need to make changes, you can go to the **Summary** page directly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. After you finish, select **Finish** to start the creation.

(Non-Citrix provisioned VDAs only) Generate and manage enrollment tokens

NOTE:

To perform this task, you must have the Cloud Administrator role.

After you decide to adopt token-based enrollment for non-Citrix provisioned machines, generate tokens on a per-machine catalog basis, and then share them with VDA installation administrators.

An enrollment token features:

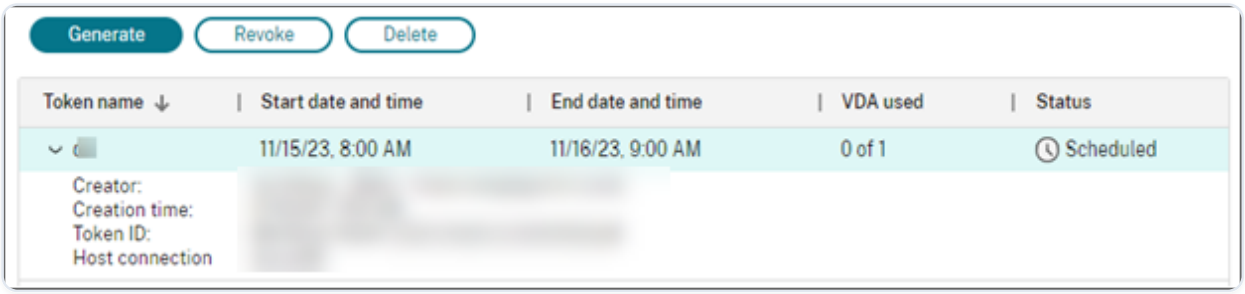
- Registration range: 1 to 5000 VDA machines
- Validity period: up to 14 days

To generate a token for a catalog using Studio, follow these steps:

1. In **Machine Catalogs**, locate a non-MCS-provisioned catalog, which has **Provisioning method: Manual** displayed in the **Machine Count** column.
2. Right-click the catalog, and then select **Manage Enrollment Tokens**.
3. On the **Generate enrollment token** page that appears, provide the following token information:
   - Type a name for the token.
   - Enter its validity period. The period must be no more than 14 days. The token is valid only for the specified period.
   - (Optional) Select a host connection for power management of VDAs enrolled with the token. Options include all host connections under this catalog's zone.
   - Enter the token usage limits (between 1–5000).
4. Click **Generate**.
5. In the **Token successfully generated** window that appears, copy the token and save it in a safe place, or click **Download** to download it to the **Downloads** folder.

   A token record appears in the token list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Share the token with VDA installation administrators.

   For more information about how to install VDA and a token on machines, see Install VDAs.

Manage tokens

You have two options to revoke a token and make it unavailable for VDA enrollment:

- Revoke: Revoke the token but retain it in the list for logging purposes.
- Delete: Revoke the token and delete it from the list.

NOTE:

Expired tokens are automatically deleted in 14 days.

Use PowerShell

This section details how you can manage catalogs using PowerShell:

- Use PowerShell to check VDA upgrade status and VDA version
- Manage the sequence number of the machine name
- Add descriptions to an image
- Reset OS disk
- Repair the identity information of active computer accounts
- Change the network setting for an existing machine catalog
- Manage versions of a machine catalog
- Change cache configuration of an existing machine catalog
- Convert a non-machine profile-based machine catalog to machine profile-based machine catalog
- Retrieve warnings and errors associated with a catalog
- Delete machines without hypervisor access

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Update properties of individual VMs

Manage the sequence number of the machine name

To customize the sequence number of machines, which are deployed using MCS, through PowerShell commands, do the following:

1. Open PowerShell as an administrator on the Delivery Controller.
2. Run the command `asnp citrix*` to load the Citrix modules.
3. Run the following command to check the start count for the identity pool of the catalog:

   ```
   Get-AcctIdentityPool -IdentityPoolName xxx
   ```

   The `IdentityPoolName` is the name of the catalog.
4. If you want to set this count to a different value, run the following command and specify the StartCount as X:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount X
   ```
5. Add the machines to the catalog so that the machines are created with the required count.
6. After creating the machines, run the following command to set it back to the original value Y:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount Y
   ```

Add descriptions to an image

You can add informative descriptions about changes related to image updates for machine catalogs. Use this feature to add a description when creating a catalog, or when you update an existing master image for a catalog. You can also display information for each master image in the catalog. This functionality is useful for administrators who want to add descriptive labels when updating a master image used by a catalog, for example, *Office 365 installed*. Use the following commands to add or view image descriptions:

- `NewProvScheme`. A new parameter, `masterImageNote` enables you to add a note to an image. For example:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName XenHu
-IdentityPoolName idPool1 -MasterImageVM XDHyp:
\HostingUnits\XenHU\Base.vm\Base.snapshot -MasterImageNote "Office365
installed"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Publish-ProvMasterVMImage`. Use this parameter to publish the note. For example:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -MasterImageVM XDHyp:\HostingUnits\HostUnit1\RhoneCC_baseXP.vm\base.snapshot -MasterImageNote "Visual Studio 2019 installed"
```

- `Get-ProvSchemeMasterVMImageHistory`. Display information for each image. For example:

`C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName MyScheme -Showall

VMImageHistoryUid : 3cba3a75-89cd-4868-989b-27feb378fec5

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

ProvisioningSchemeName : MyScheme

MasterImageVM : /Base.vm/base.snapshot

Date : 17/05/2021 09:27:50

MasterImageNote : Office365 installed`

Reset OS disk

Use the PowerShell command `Reset-ProvVMDisk` to reset the OS disk of a persistent VM in an MCS created machine catalog. Currently, this feature is applicable to AWS, Azure, Google Cloud, SCVMM, VMware, and XenServer® virtualization environments.

To successfully run the PowerShell command, make sure that:

- The target VMs are in a persistent MCS catalog.
- The MCS machine catalog is functioning properly. This implies that the provisioning scheme and host exist, and the provisioning scheme has correct entries.
- Hypervisor is not in maintenance mode.
- Target VMs are powered-off and in maintenance mode.

Perform the following steps to reset the OS disk:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run the PowerShell command `Reset-ProvVMDisk` in any one of the following ways:
    - Specify the list of VMs as a comma-separated list, and perform the reset on each VM:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
-OS
```

- Specify the list of VMs as an output from `Get-ProvVM` command, and perform the reset on each VM:

```
(Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
-OS
```

- Specify a single VM by name:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

- Create separate reset tasks for each of the VMs returned by the `Get-ProvVM` command. This is less efficient because each task will perform the same redundant checks, such as hypervisor capability check, connection check for each VM.

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
-ProvisioningSchemeName "xxx" -OS
```

4. A confirmation prompt appears that lists the VMs to be reset along with a warning message that it is an unrecoverable operation. If you do not provide an answer and press **Enter**, no further action takes place.

   You can run the PowerShell command `-WhatIf` to print the action it would take and exit without performing the action.

   You can also bypass the confirmation prompt using one of the following methods:

   - Provide the `-Force` parameter:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

   - Provide the `-Confirm:$false` parameter:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Before running the `Reset-ProvVMDisk`, change `$ConfirmPreference` to 'None':

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

NOTE:

Do not take VMs out of the maintenance mode or power them on until the completion of the reset process.

5. Run `Get-ProvTask` to get the status of the tasks returned by `Reset-ProvVMDisk` command.

Repair the identity information of active computer accounts

You can reset the identity information of active computer accounts that have identity-related problems. You can choose to reset only the machine password and trust keys, or reset all configuration of the identity disk. This implementation is applicable to both persistent and non-persistent MCS machine catalogs.

NOTE:

Currently, the feature is supported only for AWS, Azure, GCP, SCVMM, VMware, and XenServer virtualization environments.

Conditions

Ensure the following to successfully reset the identity disk:

- Turn off and set the VM to maintenance mode
- Do not include the parameter -OS in the PowerShell command

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Reset identity information

To reset identity information:

1. Open the **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Reset the identity information.

   - To reset only the machine password and trust keys, run the following command:

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     The description of the parameters used in the command is as follows:

     - `IdentityAccountName`: The name of the identity account that must be repaired.
     - `PrivilegedUserName`: User account that has write permission on identity provider (AD or Microsoft Entra ID).
     - `PrivilegedUserPassword`: Password for PrivilegedUserName.
     - `Target`: Target for the repair action. It can be IdentityInfo to repair account password/ trust key, and UserCertificate to repair user certificate attributes of Microsoft Entra hybrid joined machine identities.

   - To reset all configuration of the identity disk, run the following commands in the following order:

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     ```
     Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
     Identity
     ```

   - To completely recreate the identity disk:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
     -Identity -Recreate
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> If the machine is on a VDA version of 2511 (Update 1) or later and has the registry key set for enabling unique `MachineGuid` (`HKLM:\Software\Citrix\MachineIdentityServiceAgent\EnableUniqueMachineGuid`), it keeps using the same `MachineGuid` as before regardless of the `-Recreate` setting

4. Type **y** to confirm the action. You can also skip the confirmation prompt using the `-Force` parameter. For example:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. Run `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` to check the updated identity disk setting. The attributes of the identity disk (for example, `IdentityDiskId`) must be updated. The `StorageId` and `IdentityDiskIndex` must not change.

Change the network setting for an existing machine catalog

You can change the network setting for an existing machine catalog so that the new VMs are created on the new subnetwork. Use the parameter `-NetworkMapping` in the `Set-ProvScheme` command to change the network setting.

To change the network setting for an existing provisioning scheme, do the following:

1. In the PowerShell window, run the command `asnp citrix*` to load the PowerShell modules.
2. Run `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` to get to the network path that you want to change.
3. Assign a variable to the new network setting. For example:

```
$NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network
0.network"}
```

4. Run `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Run `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` to verify the new network setting for the existing provisioning scheme.

Manage versions of a machine catalog

When an MCS machine catalog is updated with the `Set-ProvScheme` command, the current configuration is saved as a version. You can then manage the various versions of the machine catalog using PowerShell commands. You can:

- See the list of versions of a machine catalog.
- Use any previous version to update the machine catalog.
- Manually delete a version if it is not used by a VM of that machine catalog.
- Change the maximum number of versions to be retained by the machine catalog (the default is 99).

A version includes the following information of a machine catalog:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Run the following commands (provided as examples) to manage the various versions of a machine catalog.

- To see the configuration details of the various versions of a machine catalog:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- To see the configuration details of a particular version of a machine catalog:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- To see the total number of versions associated with a machine catalog:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- To use any previous version to update the machine catalog:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- To manually delete a version if it is not used by a VM of that machine catalog:

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- To set the maximum number of versions to be retained by the machine catalog (the default is 99). This setting is applied across all the catalogs. For example, in this case, a maximum of 15 versions will be retained for all the MCS provisioned catalogs.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

If the number of versions reaches the maximum number of versions, then a new version cannot be created if older versions are in use by any of the VMs in the machine catalog. In that case, do one of the following:

- Increase the limit of the maximum number of versions to be retained by the machine catalog.
- Update some VMs that are on older versions so that those older versions are no longer referenced by any VMs, and can be deleted.

Change cache configuration of an existing machine catalog

After creating a non-persistent catalog with MCSIO enabled, you can use the `Set-ProvScheme` command to modify the following parameters:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

This feature is currently applicable to:

- GCP and Microsoft Azure environments, and
- a non-persistent catalog with MCSIO enabled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements

The requirements to modify the cache configuration are:

- Update to the latest version of VDA (2308 or later).
- Enable the parameter `UseWriteBackCache` for the existing machine catalog. Use `New-ProvScheme` to create a machine catalog with `UseWriteBackCache` enabled. For example:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

Change the cache configuration

Run the `Set-ProvScheme` command. For example:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

NOTE:

- The value of `WriteBackCacheDiskSize` must be more than zero because at least 1 GB of cache disk storage is required.
- The value of `WriteBackCacheMemorySize` must be less than the machine catalog memory size.
- These changes only affect new VMs added to the catalog after the change is made. Existing VMs are not affected by these changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Convert a non-machine profile-based machine catalog to a machine profile-based machine catalog

You can use a VM, template spec (in case of Azure), or launch template (in case of AWS), or VMware template (in case of VMware) as a machine profile input to convert a non-machine profile-based machine catalog to machine profile-based machine catalog. New VMs added to the catalog take property values from the machine profile.

NOTE:

An existing machine profile-based machine catalog cannot be changed to a non-machine profile-based machine catalog.

To do this:

1. Create a persistent or non-persistent machine catalog with VMs and without a machine profile.
2. Open the **PowerShell** window.
3. Run the `Set-ProvScheme` command to apply the property values from the machine profile to the new VMs added to the machine catalog. For example:
   - In the case of Azure:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
     \HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
     Name>\<TemplateSpecName>\<VersionName>
     ```

   - In the case of AWS:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
     \HostingUnits\<hosting-unit>\<launch-
     template>.launchtemplate\<launch-template-
     version>.launchtemplateversion"
     ```

   - In the case of VMware:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-prov-scheme"
     -MachineProfile "XDHyp:\HostingUnits\my-hosting-unit\my-
     template.template"
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Set the `FolderID` as the custom property to avoid deriving `FolderID` from the VMware template.

Retrieve warnings and errors associated with a catalog

You can get historical errors and warnings to understand issues with your MCS machine catalog and fix those issues.

Using PowerShell commands, you can:

- Get a list of errors or warnings
- Change the warning state from **New** to **Acknowledged**
- Delete the errors or warnings

To run the PowerShell commands:

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.

To get a list of errors and warnings:

Run `Get-ProvOperationEvent` command.

- With no parameters: Gets all errors and warnings
- With `LinkedObjectType` and `LinkedObjectUid` parameter: Gets all errors and warnings associated with a specific provisioning scheme
- With `EventId` parameter: Gets a specific error or warning that matches this event ID
- With `Filter` parameter: Gets errors or warnings by a customized filter

To change the state of errors or warnings from **New** to **Acknowledged**:

Run `Confirm-ProvOperationEvent` command.

- With `EventId` parameter: Sets the state of a specific error or warning that matches this event ID. You can get the `EventId` of a specific error or warning as an output from `Get-ProvOperationEvent` command
- With `LinkedObjectType` and `LinkedObjectUid` parameters: Sets the state of all the errors and warnings associated with a specific provisioning scheme

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- With `All` parameter: Sets the state of all errors and warnings as **Acknowledged**

To delete the errors or warnings:

Run `Remove-ProvOperationEvent` command.

- With `EventId` parameter: Removes a specific error or warning that matches this event ID. You can get the `EventId` of a specific error or warning as an output from `Get-ProvOperationEvent` command
- With `LinkedObjectType` and `LinkedObjectUid` parameters: Removes all errors and warnings associated with a specific provisioning scheme
- With `All` parameter: Removes all errors and warnings

For more information, see the Citrix PowerShell SDK.

Delete machines without hypervisor access

When deleting a VM or a provisioning scheme, MCS needs to remove tags from the VM, and sometimes from the base disk as well, so that the resources included in the deletion options are no longer tracked or identified by MCS. However, some of these resources are only accessible through hypervisor. Use the `PurgeDBOnly` option in `Remove-ProvVM` PowerShell to delete VM resource objects such as VM, base disk, image in ACG, and so on from the database even when there is no hypervisor access.

This option is enabled on:

- all supported hypervisors
- persistent and non-persistent VMs

Limitations

You cannot use the commands -PurgeDBOnly and -ForgetVM at the same time.

Use the PurgeDBOnly command

When running the PowerShell command `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` the deletion operation might fail in the following scenarios:

- The host connection is in maintenance mode
- Invalid credentials
- Authentication failure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Unauthorized operation
- The hypervisor is unreachable

NOTE:

Remove-provVM -ForgetVM targets only persistent VMs. If one of the VMs in the list is non-persistent, the operation fails.

When the operation fails because the hypervisor is unreachable, the following prompt appears:

```
Try to use -PurgeDBOnly option to clean DDC database.
```

Use the `-PurgeDBOnly` option in the `Remove-ProvVM` PowerShell command to delete references of a VM from MCS database. For example,

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

Update properties of individual VMs

You can update properties of individual VMs in a persistent MCS machine catalog using the PowerShell command `Set-ProvVM`. However, the updates are not applied immediately. You must set the time window using the PowerShell command `Set-ProvVMUpdateTimeWindow` for the updates to apply.

This implementation helps you to manage individual VMs efficiently without updating the entire machine catalog. Currently, this feature is applicable to Azure and VMware environments.

Currently, the properties that you can update are:

- `CustomProperties`
- `ServiceOffering` (Not applicable to VMware)
- `MachineProfile`
- `CpuCount`
- `Memory`

Using this feature, you can:

- Update the properties of a VM
- Retain the properties updated on a VM after the machine catalog is updated
- Revert the configuration updates applied to a VM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Before updating properties of a VM:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Check the configuration of the existing machine catalog. For example:

   ```
   Get-ProvScheme -ProvisioningSchemeName <catalog name>
   ```

4. Check the configuration of the VM on which you want to apply the updates. For example:

   ```
   Get-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
   ```

Update properties of a VM

Do the following to update the properties on a VM:

1. Turn off the VM on which you want to apply the updates.
2. Update the properties of the VM. For example, if you want to update storage type (`StorageType`) custom property of the VM, run the following:

   ```
   Set-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
   -CustomProperties "...<Property Name='StorageType'
   Value='Premium_LRS' />..."
   ```

   You can update properties of two VMs in a machine catalog simultaneously. For example:

   ```
   Set-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
   -CustomProperties "...<Property Name='StorageType'
   Value='Premium_LRS' />..."
   ```

   ```
   Set-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine2
   -CustomProperties "...<Property Name='StorageType'
   Value='StandardSSD_LRS' />..."
   ```

   NOTE:

   The updates are not applied immediately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Get the list of properties that are specified to be updated and the configuration version. For example:

   ```
   Get-ProvVMConfiguration -ProvisioningSchemeName <catalog name> -VMName
   machine1
   ```

   Check the property value of `Version` and the properties to be updated (in this case, `StorageType`).

4. Check the configuration version. For example:

   ```
   Get-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
   ```

   Check the property value of `ProvVMConfigurationVersion`. The update is not yet applied. The VM is still in the old configuration.

5. Request scheduled update. For example:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <catalog name>
   -StartsNow -DurationInMinutes -1
   ```

   For more information on scheduled updates, see Update provisioned machines to current provisioning scheme state.

   NOTE:

   Any pending provisioning scheme update is also applied.

6. Restart the VM. For example:

   ```
   New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
   ```

7. Check the configuration version. For example:

   ```
   Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
   ```

   Check the property value of `ProvVMConfigurationVersion`. The update is now applied. The VM now has the new configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. To apply further configuration updates on the VM, turn off the VM, and repeat the steps.

Retain the properties updated on a VM after the machine catalog is updated

Do the following to retain the properties updated on a VM:

1. Turn off the VM on which you want to apply the updates.
2. Update the machine catalog. For example, if you want to change the VM size (`ServiceOffering`) and storage type (`StorageType`), run the following:

   ```
   Set-ProvScheme -ProvisioningSchemeName <catalog name> -ServiceOffering
   Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
   Value='StandardSSD_LRS' />..."
   ```

3. Get the configuration details of the machine catalog. For example:

   ```
   Get-ProvScheme -ProvisioningSchemeName <catalog name>
   ```

   The `ProvisioningSchemeVersion` is now incremented by one. The VM size and storage type are also updated.

4. Update the properties of the VM. For example, provide a machine profile to the VM.

   ```
   Set-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
   -MachineProfile "XDHyp:\HostingUnits\<hosting-
   unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
   spec>.templatespec\<template-spec-version>.templatespecversion"
   ```

   NOTE:

   The machine profile input has a tag and a different VM size (`ServiceOffering`) specified.

5. Get the list of properties that the VM will have after merging the configuration updates on the VM with the machine catalog updates. For example:

   ```
   Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName <catalog
   name> -VMName machine1
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Any updates on the VM will override the updates done on the machine catalog.

6. Request scheduled update for the VM. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <catalog name>
-VMName machine1 -StartsNow -DurationInMinutes -1
```

7. Restart the VM. For example:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

   The VM keeps its updated VM size as derived from the machine profile. The tag values as specified in the machine profile are also applied to the VM. However, the storage type is derived from the latest provisioning scheme.

8. Get the configuration version of the VM. For example:

```
Get-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
```

   The `ProvisioningSchemeVersion` and `ProvVMConfigurationVersion` now shows the latest version.

Revert the configuration updates applied to a VM

1. After applying the updates to a VM, turn off the VM.
2. Run the following command to remove the updates that are applied on the VM. For example:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
<catalog name> -VMName machine1
```

3. Request scheduled update for the VM. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <catalog name>
-VMName machine1 -StartsNow -DurationInMinutes -1
```

4. Restart the VM. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. Check the configuration version of the VM. For example:

   ```
   Get-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
   ```

   The `ProvVMConfigurationVersion` value is now the configuration version of the machine catalog.

Storage migration of VMs

You can move the disk storage of existing VMs from an old storage to a new storage in VMware and XenServer environments. During migration, MCS retains the VM capabilities such as power management, reset OS disk, and so on. You can also add new VMs to the machine catalog using the new disk storage. To do this, use the PowerShell command `Move-ProvVMDisk`.

You can migrate full clone persistent VMs and non-persistent VMs.

- For persistent Full Clone VMs: OS Disk, Identity Disk, and non-MCS provisioned disks.
- For non-persistent VMs: OS Disk, Identity Disk, and Write-back Cache (WBC) disk.

The new storage must satisfy the following conditions:

- It must be within the same cluster of the old storage.
- The host on which the VM is running must have access to both the old and new datastores.

Migrate the disk storage

To migrate the disk storage:

1. Add a destination storage to an existing hosting unit. You can run the PowerShell command `Add-Hyphostingunitstorage` to add the destination storage:

   If you do not want to add new VMs to the old storage, then change the old storage to **Superseded**. You can do this using Studio or PowerShell commands. For Studio, see Edit storage. Alternatively, run `Set-Hyphostingunitstorage` and set `Superseded` as `true` to disable new VM creation in the old storage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For non-persistent VMs:

- If WBC is used, then configure the WBC destination storage in the hosting unit.
- If OS destination storage is configured, then WBC (if used) must be compatible with OS destination storage.
- If OS destination storage is not configured, then WBC (if used) must be compatible with the current OS storage.

2. Turn off the VMs and turn on the **Maintenance Mode**.
3. Get the information about the provisioning scheme, hosting unit, OS disk storage, and WBC disk storage.
   - Run `ProvResourceInStorage` for OS storage information. For example:

     ```
     $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
     xxxxx

     $result

     $result.ProvResourceInStorage | Format-List -Property *
     ```

   - Run `TemporaryStorageInfo` for WBC storage information. For example:

     ```
     $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
     xxxxx

     $result

     $result.TemporaryStorageInfo | Format-List -Property *
     ```

4. Migrate the OS disk, Identity disk, and WBC disk (applicable to non-persistent VMs) to the destination storage using the `Move-ProvVMDisk` PowerShell command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Always provide the OS and Identity disks in the DiskType and `DestinationStorageId` parameters.
- The `DestinationStorageId` for OS disk and Identity disk must be the same.

Example:

Persistent VMs:

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myFullCloneProvScheme" -VMName "machine01"
-DiskType OS,Identity -DestinationStorageId datastore1,datastore1
```

IMPORTANT:

For persistent VM, all disks are moved. You cannot select which disks to move.

Non-persistent VMs:

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myCleanOnBootProvScheme" -VMName "machine01"
-DiskType OS,Identity,WBC -DestinationStorageId None,None,datastore1
```

IMPORTANT:

- If you don't want to migrate a specific disk, set the value as `None` for the `DestinationStorageId` parameter.
- If the VM has WBC disk, then add the WBC disk in `DiskType` parameter and add the required information in `DestinationStorageId` parameter.

Troubleshoot

If one of the disks fails to migrate, then none of the disks are migrated to the destination storage. You can get the failure report using the following command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines
```

Important considerations for migration of non-persistent VMs in VMware

- If you try to move the OS and Identity disk to a new storage, the VM specific files are also moved to the new storage.
- VMware doesn't support moving the disk if it has the snapshot.

Migrate existing MCS provisioned catalogs to prepared image machine catalog

You can convert an existing MCS provisioned machine catalog into a prepared image machine catalog using a PowerShell command `Set-ProvSchemeImage`. However, you cannot revert to the legacy catalog after migration. Currently, this feature is applicable to Azure and VMware virtualization environments.

Limitations

Consider the following limitations:

- If the MCS catalog uses a persistent data disk, the catalog cannot be migrated to use a prepared image.
- If the MCS catalog uses unmanaged disks, the catalog cannot be migrated to use a prepared image.

Migrate to prepared image machine catalog

To migrate, do the following:

1. Create an image definition and image versions using Studio or PowerShell commands. See the steps to create image definitions and image versions in:
    - Azure:
        - Studio
        - PowerShell
    - VMware:
        - Studio
        - PowerShell

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Run `Get-ProvScheme` command to get the provisioning scheme UID. For example:

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid
```

3. Run `Get-ProvImageVersionSpec` command to get the Image definition name, image version spec uid. For example:

```
Get-ProvImageVersionSpec -ImageDifinitionName <name> -Filter
{IsPrepared -eq $true} | select ImageDefinitionName ImageVersionSpecUId
```

4. Run `Set-ProvSchemeImage` command to migrate an existing MCS provisioned machine catalog into a prepared image machine catalog. For example:

```
Set-ProvSchemeImage -ProvisioningSchemeName [ProvisioningSchemeName]
-ImageVersionSpecUid [ImageVersionSpecUid]
```

5. Run `Get-ProvScheme` command to check that the catalog is migrated. For example:

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid, ImageVersionSpecUid
```

Troubleshoot

- For machines with `Power State Unknown` status, see CTX131267 for guidance.
- To fix VMs that continuously show an unknown power state, see How to fix VMs that continuously show an unknown power state.
- If a Cloud Connector is not operating properly, MCS provisioning operations (such as catalog updates) take longer than usual and the management console performance degrades significantly.

Where to go next

For information on managing specific hypervisor catalogs, see:

- Manage an AWS catalog
- Manage a Google Cloud Platform catalog
- Manage a Microsoft Azure catalog

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Manage a Microsoft System Center Virtual Machine Manager catalog
- Manage a VMware catalog
- Manage a XenServer catalog

Manage an AWS EC2 catalog

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to AWS EC2 cloud environments.

NOTE:

Before managing an AWS catalog, you need to finish creating an AWS catalog. See Create an AWS EC2 catalog.

Remove tags

When you create a catalog or a VM, tags are created on the following resources:

- Virtual machine
- Root disk volume
- Identity disk volume
- Elastic network interface (ENI)
- Root disk image (AMI)
- Launch template
- Snapshot of AMI or root disk

You can remove VMs and machine catalogs from Citrix® database and remove Citrix-created tags. You can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and Citrix-created tags from a single VM or a list of VMs from a machine catalog.

  NOTE:

  With the `ForgetVM` parameter, the VMs are removed from the Citrix's provisioning scheme database, however, the VMs continue to remain in the hypervisor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Remove-ProvScheme` with `ForgetVM` parameter to remove a machine catalog from the Citrix database and resources from a machine catalog.

To do this:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Unlock the VM before removing the VMs. For example:

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. Run one of the following commands to remove VMs, machine catalog, and Citrix-created tags from resources.

   - Run `Remove-ProvVM` with `ForgetVM` to remove VMs from Citrix database and Citrix-created tags from VMs. For example:

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

   - Run `Remove-ProvScheme` to remove machine catalog from Citrix database and resources from a machine catalog. For example:

     ```
     Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
     ```

5. Verify that the VM is removed from the Delivery Controller™, but, not from the hypervisor.

   a. Run `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`. This must return nothing.

   b. Go to AWS EC2 console. You must see the VMs, however, the Citrix-created tags are now removed. Citrix-created tags from the following resources are removed:

      - Virtual machine
      - Root disk volume
      - Identity disk volume
      - ENI

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. If you remove the machine catalog, verify that the catalog is removed from the Delivery Controller.

    a. Run `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. This must return an error.

    b. Verify in AWS EC2 console that the following resources are removed.

    - Root disk image (AMI)
    - Launch template
    - Snapshot of AMI or root disk

Identify resources created by MCS

Following are the tags that MCS adds to the resources on AWS platform. The tags in the table are represented as "key":"value".

RESOURCE NAME	TAG
ID disk	"Name": "VMName_IdentityDisk"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Image	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ENI	"Description": "XD Nic"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OS disk	"Name": "VMName_rootDisk"
	"XdConfig": "XdProvisioned=True"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE NAME	TAG
	[when AwsCaptureInstanceProperties = true] "Citrix Resource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
PrepVM	"Name": "Preparation - CatalogName - xxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix Resource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
Published snapshot	"XdConfig": "XdProvisioned=true"
	If not a snapshot for Volume Worker AMI, then "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Template	[when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=true"
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE NAME	TAG
VM in catalog	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx"
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
Volume worker AMI	"XdConfig": "XdProvisioned=true"
Volume worker bootstraper	"Name": "XenDesktop® Temp"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": ""
Volume worker instance	"Name": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"
	"XdConfig": "XdProvisioned=true"

Convert legacy MCS catalogs in AWS to machine profile-based catalogs

To convert a non-machine profile-based machine catalog to a machine profiled-based machine catalog, complete the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. On the **Machine Catalogs** page, right-click the **Machine Catalog** name that you want to convert, and then select **Edit Machine Catalog**.
2. On the **Edit Machine Catalog > Machine Profile** page, select the **Use a machine profile** check box.
3. Click **Select a machine profile**.
4. On the **Select a machine profile** page, select a virtual machine or launch template to use as the machine profile.
5. If some current settings differ from the new machine profile settings, select the required option for the settings you want to use and click **Continue**.
6. Click **Apply**.

More information

- Create and manage connections and resources
- Connection to AWS EC2
- Create machine catalogs
- Create an AWS EC2 catalog
- Manage machine catalogs

Manage a catalog of Amazon WorkSpaces Core Managed Instances

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to Amazon WorkSpaces Core Managed Instances.

NOTE:

Before managing a catalog of Amazon WorkSpaces Core Managed Instances, you need to finish creating a catalog of Amazon WorkSpaces Core Managed Instances. See Create a catalog of Amazon WorkSpaces Core Managed Instances.

Remove tags

When you create a catalog or a VM, tags are created on the following resources:

- Virtual machine
- Root disk volume
- Identity disk volume

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Elastic network interface (ENI)
- Root disk image (AMI)
- Launch template
- Snapshot of AMI or root disk

You can remove VMs and machine catalogs from Citrix® database and remove Citrix-created tags. You can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and Citrix-created tags from a single VM or a list of VMs from a machine catalog.

  NOTE:

  With the `ForgetVM` parameter, the VMs are removed from the Citrix's provisioning scheme database, however, the VMs continue to remain in the hypervisor.

- `Remove-ProvScheme` with `ForgetVM` parameter to remove a machine catalog from the Citrix database and resources from a machine catalog.

To do this:

1. Open a **PowerShell** window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Unlock the VM before removing the VMs. For example:

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. Run one of the following commands to remove VMs, machine catalog, and Citrix-created tags from resources.

   - Run `Remove-ProvVM` with `ForgetVM` to remove VMs from Citrix database and Citrix-created tags from VMs. For example:

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

   - Run `Remove-ProvScheme` to remove machine catalog from Citrix database and resources from a machine catalog. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. Verify that the VM is removed from the Delivery Controller™, but, not from the hypervisor.
   a. Run `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`. This must return nothing.
   b. Go to AWS EC2 console. You must see the VMs, however, the Citrix-created tags are now removed. Citrix-created tags from the following resources are removed:
      - Virtual machine
      - Root disk volume
      - Identity disk volume
      - ENI
6. If you remove the machine catalog, verify that the catalog is removed from the Delivery Controller.
   a. Run `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. This must return an error.
   b. Verify in AWS EC2 console that the following resources are removed.
      - Root disk image (AMI)
      - Launch template
      - Snapshot of AMI or root disk

Identify resources created by MCS

Following are the tags that MCS adds to the resources on AWS platform. The tags in the table are represented as "key":"value".

RESOURCE NAME	TAG
ID disk	"Name": "VMName_IdentityDisk"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE NAME	TAG
Image	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ENI	"Description": "XD Nic"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OS disk	"Name": "VMName_rootDisk"
	"XdConfig": "XdProvisioned=True"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"Name": "Preparation - CatalogName - xxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Published snapshot	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Template	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM in catalog	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More information

- AWS virtualization environments
- Connection to Amazon WorkSpaces Core Managed Instances
- Image management
- Create a prepared image for Amazon WorkSpaces Core Managed Instances
- Create a catalog of Amazon WorkSpaces Core Managed Instances
- Manage prepared image machine catalogs

Manage a Google Cloud Platform catalog

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to Google cloud environments.

NOTE:

Before managing a Google Cloud Platform catalog, you need to finish creating a Google Cloud Platform catalog. See Create a Google Cloud Platform catalog.

Add machines to a catalog

To add machines to a catalog, follow these steps:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select the machine catalog to which you want to add machines.
3. Select **Add Machines** in the action bar.
4. On the **Virtual Machines** page, specify the number of machines you want to add and then select **Next**.
5. On the **Machine Identities** page, select an Active Directory account and then select **Next**.
6. On the **Domain Credentials** page, select **Enter credentials**, type the user name and password, select **Save**, and then select **Next**.
7. On the **Summary** page, confirm the information and then select **Finish**.

Update machines

This feature can be useful in cases where you want to update your master image or the minimum functional level.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To update machines, follow these steps:

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select the machine catalog that contains machines you want to update.
3. Select **Change Master Image** in the action bar.
4. On the **Image** page, select a VM and the minimum functional level for the catalog and then select **Next**.
5. On the **Rollout Strategy** page, specify when you want to update the machines and then select **Next**.
6. On the **Summary** page, confirm the information and then select **Finish**.

Roll back a machine update

To roll back a machine update, follow these steps:

IMPORTANT:

Do not rename, delete, or move master images. Otherwise you cannot roll back the update.

1. From Studio, select **Machine Catalogs** in the left pane.
2. Select the machine catalog where you want to roll back the machine update.
3. Select **Roll Back Master Image** in the action bar.
4. On the **Overview** page, confirm the information and then select **Next**.
5. On the **Rollout Strategy** page, configure the rollout strategy and then select **Next**.
6. On the **Summary** page, confirm the information and then select **Finish**.

Power management

Citrix DaaS™ lets you do the power management of Google Cloud machines. Use the **Search** node in the navigation pane to locate the machine you want to power manage. The following power actions are available:

- Delete
- Start
- Restart
- Force Restart
- Shut Down

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Force Shutdown
- Add to Delivery Group
- Manage Tags
- Turn On Maintenance Mode

You can also power manage Google Cloud machines by using Autoscale. To do so, add the Google Cloud machines to a Delivery Group and then enable Autoscale for that Delivery Group. For more information about Autoscale, see Autoscale.

Update provisioned machines using PowerShell

The `Set-ProvScheme` command changes the provisioning scheme. However, it does not affect existing machines. Using the PowerShell command `Set-ProvVMUpdateTimeWindow`, you can now apply the current provisioning scheme to an existing persistent or non-persistent machine or set of machines. Currently, in GCP, the property updates supported by this feature are Machine profile, Service offering and Custom catalog settings.

You can update:

- A single VM
- A list of specific VMs or all existing VMs associated with a provisioning scheme ID
- A list of specific VMs or all existing VMs associated with a provisioning scheme name

To update the existing VMs:

1. Check the configuration of the existing machines. For example,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. Update the provisioning scheme. For example,

   - Updating machine profile

     ```
     `Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
     "XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
     ```

   - Updating service offering

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
“XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

3. Check if the current property of the VM matches the current provisioning scheme, and if there is any pending update action on the VM. For example,

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   You can also find machines with a particular version. For example,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
   ProvisioningSchemeVersion
   ```

4. Update existing machines.

   - To update all the existing machines:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - To update a list of specific machines:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - To update machines based on the output of `Get-ProvVM`:

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- `StartsNow` indicates that the scheduled start time is the current time.
- `DurationInMinutes` with a negative number (for example, –1) indicates no upper bound on the schedule's time window.

5. Find machines with an update scheduled. For example,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. Restart the machines. At the next power-up, property changes are applied to the existing machines. You can check the updated status using the following command:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Change disk related custom properties of an existing catalog

You can change the following disk related custom properties of an existing catalog and existing VMs of the catalog:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

NOTE:

- `StorageType` property is for OS disk
- `PersistOsDisk` property can be set only for non-persistent catalog with write-back cache enabled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This implementation helps you to select different storage types for different disks even after you create a catalog and thus, balances pricing associated with different storage types.

To do this, use PowerShell commands `Set-ProvScheme` and `Set-ProvVMUpdateTimeWindow`:

1. Open a **PowerShell** window.
2. Run `asnp citrix*`.
3. Run `Get-ProvVM -VMName <VM name>` to get the custom properties.
4. Change the custom properties string:
   a. Copy the custom properties to a Notepad and change the custom properties.
   b. In the **PowerShell** window, paste the modified custom properties from Notepad and assign a variable to the modified custom properties. For example:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. Update the existing catalog. For example:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. Update the existing VMs. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. Restart the VMs. At the next power up, custom property changes are applied to the existing VMs.

Protect accidental machine deletion

Citrix DaaS lets you protect MCS resources on the Google Cloud to prevent accidental deletion. Configure the provisioned VM by setting the `deletionProtection` flag to TRUE.

By default, VMs provisioned through MCS or Google Cloud plug-in are created with InstanceProtection enabled. The implementation is applicable to both persistent and non-persistent catalogs. The non-persistent catalogs are updated when the instances get re-created from the template. For existing persistent machines, you can set the flag in the Google Cloud console. For more information about setting the flag, see the Google Documentation site. New machines added to persistent catalogs are created with `deletionProtection` enabled.

If you attempt to delete a VM instance for which you have set the `deletionProtection` flag, the request fails. However, if you are granted the permission `compute.instances.setDeletionProtection` or assigned the IAM **Compute Admin** role, you can reset the flag to allow the resource to be deleted.

Identify resources created by MCS

Following are the tags that MCS adds to the resources on GCP platform. The tags in the table are represented as "key":"value".

RESOURCE NAME	TAG
ID disk	"CitrixResource": "internal"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Image	"CitrixResource": "internal"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OS disk	"CitrixResource": "internal"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE NAME	TAG
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Preparation VM	"CitrixResource": "internal"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Published snapshot	"CitrixResource": "internal"
Storage bucket	"CitrixResource": "internal"
Template	"CitrixResource": "internal"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM in catalog	"CitrixResource": "internal"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". The plug-in also adds this label for MCS provisioned VMs: "citrix-provisioning-scheme-id": "provSchemeId". You can use this label to filter by catalog in the GCP console.
WBC disk	"CitrixResource": "internal"
	CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

NOTE:

A VM is not visible in the Citrix inventory if a **CitrixResource** tag is added to identify it as a resource created by MCS. You can remove or rename the tag to make it visible.

More information

- Create and manage connections and resources
- Connection to Google cloud environments

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Create machine catalogs
- Create a Google Cloud Platform catalog
- Manage machine catalogs

Manage an HPE Moonshot catalog

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to HPE Moonshot catalog.

NOTE:

Before managing a HPE Moonshot catalog, you need to finish creating a HPE Moonshot catalog. See Create an HPE Moonshot machine catalog.

Power management

Citrix DaaS™ lets you do power management of HPE Moonshot machines. Use the **Search** node in the navigation pane to locate the machine you want to power manage. The following power actions are available:

- Start
- Shut Down
- Force Shutdown
- Restart
- Reset

NOTE:

Suspend and **Resume** power actions are not supported.

More information

- Create and manage connections and resources
- Connection to HPE Moonshot
- Create machine catalogs
- Create an HPE Moonshot machine catalog
- Manage machine catalogs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage a Microsoft Azure catalog

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to Microsoft Azure Resource Manager cloud environments.

NOTE:

Before managing a Microsoft Azure catalog, you need to finish creating a Microsoft Azure catalog. See Create a Microsoft Azure catalog.

Change the storage type to a lower tier when a VM is shut down

You can save storage costs by switching the storage type of a managed disk to a lower tier when you shut down a VM. To do this, use the `StorageTypeAtShutdown` custom property.

The storage type of the disk changes to a lower tier (as specified in the `StorageTypeAtShutdown` custom property) when you shut down the VM. After you power on the VM, the storage type changes back to the original (as specified in `StorageType` custom property or `WBCDiskStorageType` custom property).

IMPORTANT:

- The disk does not exist until the VM is powered on at least once. Therefore, you cannot change the storage type when you first power on the VM.
- A VM might take a little longer to start after you change the storage type to a lower tier.

Requirements

- Applicable to a managed disk. This implies that you set the custom property `UseManagedDisks` to true.
- Applicable to a persistent and non-persistent catalog with a persistent OS disk. This implies that you set the custom property `persistOsDisk` to true.
- Applicable to a non-persistent catalog with a persistent WBC disk. This implies that you set the custom property `persistWBC` to true.

Restriction

- As per Microsoft, you can only change the disk type twice per day. See the Microsoft document. As per Citrix, the `StorageType` update happens whenever there is a Start or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deallocate action for the VM. Therefore, limit the number of power actions per VM to twice per day. For example, one power action in the morning to start the VM and one in the evening to deallocate the VM.

Change the storage type to a lower tier

Before proceeding with the steps, see the Requirements and Restrictions.

1. Add the custom property `StorageTypeAtShutdown`, set the value to Standard_LRS (HDD), and create a catalog using `New-ProvScheme`.

   NOTE:

   If `StorageTypeAtShutdown` has any value other than empty or Standard_LRS (HDD), the operation fails.

   Example of setting custom properties while creating a persistent catalog:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS“ />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</CustomProperties>’
```

Example of setting custom properties while creating a non-persistent catalog:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>’
```

NOTE:

When you use a machine profile, the custom property takes precedence over the property defined in `MachineProfile`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Shut down the VM and check the storage type of the VM in Azure portal. The storage type of the disk changes to a lower tier, as specified in the `StorageTypeAtShutdown` custom property.
3. Turn on the VM. The storage type of the disk switches back to the storage type mentioned in:
    - `StorageType` custom property for OS disk
    - `WBCDiskStorageType` custom property for WBC disk only if you specify it in `CustomProperties`. Otherwise, it switches back to the storage type mentioned in `StorageType`.

Apply `StorageTypeAtShutdown` to an existing catalog

Before proceeding with the steps, see the Requirements and Restrictions.

Use `Set-ProvScheme` to apply `StorageTypeAtShutdown` to the new VMs added to an existing catalog.

Example of setting custom properties while adding a VM to an existing catalog:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>’



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

Change the storage type of existing VMs to a lower tier on shutdown

Before proceeding with the steps, see the Requirements and Restrictions.

You can save storage costs by changing the storage type of existing VMs to a lower tier when the VMs are shut down.

To change the Storage type of existing machines in a catalog to a lower tier when the VMs are shut down:

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Run `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Change the custom properties string.

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Update the provisioning scheme of the existing catalog. The update applies to new VMs added after running `Set-ProvScheme`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. Update the existing VMs to enable `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

7. When you power on the machines next time, the `StorageTypeAtShutdown` property of the machines is updated. The storage type changes at the next shutdown.
8. Run the following command to view the `StorageTypeAtShutdown` value for each VM in a catalog.

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

Convert legacy MCS catalogs in Azure to machine profile-based catalogs

To convert a non-machine profile-based machine catalog to a machine profiled-based machine catalog, complete the following steps:

1. On the **Machine Catalogs** page, right-click the **Machine Catalog** name that you want to convert, and then select **Edit Machine Catalog**.
2. On the **Edit Machine Catalog** > **Machine Profile** page, select the **Use a machine profile (mandatory for Microsoft Entra ID)** checkbox.
3. Click **Select a machine profile**.
4. On the **Select a machine profile** page, select a virtual machine or launch template to use as a machine profile.
5. If some current settings differ from the new machine profile settings, select the required option for the settings you want to use and click **Continue**.
6. Click **Apply**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Update provisioned machines to current provisioning scheme state

The `Set-ProvScheme` command changes the provisioning scheme. However, it does not affect existing machines. Using the PowerShell command `Set-ProvVMUpdateTimeWindow`, you can apply the current provisioning scheme to an existing persistent or non-persistent machine or set of machines. You can also schedule a time slot for the configuration updates of the existing MCS provisioned machines. Any power on or restart during the scheduled time slot applies a scheduled provisioning scheme update to a machine. Currently, in Azure, you can update `ServiceOffering`, `MachineProfile`, and the following custom properties:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`
- `Zones`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- You can only update `StorageType`, `WBCDiskStorageType`, and `IdentityDiskStorageType` custom properties for a catalog using managed disk in Azure environments.
- If you run `Set-ProvVMUpdateTimeWindow` twice, then the most recent command takes effect.
- If a VM is updated with `Set-ProvVMUpdateTimeWindow` and the current availability zones list provided by the Zones custom property was changed to not include the zone the VM is currently using, then the VM's persistent disks will be copied to the new zone and originals deleted. For instance, a VM provisioned in zone 3 updated with the Zones custom property set to "1,2" will move the VM and its disks to either zone 1 or 2, depending on which of the two zones has less machines to balance machines between zones 1 and 2.
- If the Zones custom property is cleared entirely (set to an empty value), the VM's zone affinity is removed, allowing Azure to place the VM in any availability zone based on capacity. In this case, the VM's persistent disks remain in their original zone and are not moved.

You can update:

- A single VM
- A list of specific VMs or all existing VMs associated with a provisioning scheme ID
- A list of specific VMs or all existing VMs associated with a provisioning scheme name (machine catalog name)

After you make the following changes to the provisioning scheme, VM instance gets recreated for persistent catalogs in Azure:

- Change the `MachineProfile`
- Remove `LicenseType`
- Remove `DedicatedHostGroupId`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The OS disk of existing machines along with all its data remains as is and a new VM is attached to the disk.

Before updating the existing VMs:

1. Check the configuration of the existing machines. For example,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. Update the provisioning scheme. For example,

   - With VM as a machine profile input:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
group>.resourcegroup\<virtual-machine>.vm"
```

   - With template spec as a machine profile input:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"

-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-
group>.resourcegroup\<template-spec>.templatespec\<template-spec-
version>.templatespecversion"

-ServiceOffering "XDHyp:\HostingUnits\<hosting-
unit>\serviceoffering.folder\<service-offering>.serviceoffering"
```

   - With just service offering:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
"XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Check if the current property of the VM matches the current provisioning scheme, and if there is any pending update action on the VM. For example,

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   You can also find machines with a particular version. For example,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
   ProvisioningSchemeVersion
   ```

To request updates for existing machines to apply at the next restart:

1. Run the following commands to update existing machines and have the updates apply at the next restart.

   - To update all the existing machines. For example,

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - To update a list of specific machines. For example,

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - To update machines based on the output of Get-ProvVM. For example,

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- `StartsNow` indicates that the scheduled start time is the current time.
- `DurationInMinutes` with a negative number (for example, –1) indicates no upper bound on the schedule's time window.

2. Find machines with an update scheduled. For example,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. Restart the machines. At the next power-up, property changes are applied to the existing machines. You can check the updated status using the following command. For example,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

To schedule a VM to update to the latest provisioning settings next time it starts in the scheduled time window:

1. Run the following commands:

   - To schedule an update with start time as the current time:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName vm1 -StartsNow -DurationInMinutes 120
```

   - To schedule an update on a weekend:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
(New –TimeSpan –Days 2).TotalMinutes
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- `VMName` is optional. If not specified, the update is scheduled for the entire catalog.
- Instead of `StartTimeInUTC`, use `StartsNow` to indicate that the schedule start time is the current time.
- `DurationInMinutes` is optional. The default is 120 minutes. A negative number (for example, –1) indicates no upper bound on the schedule's time window.

2. Check the update status.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. Power on the VM. If you power on the machine after the scheduled time slot, configuration update is not applied. If you power on the machine within the scheduled time slot,
   - If the machine is powered off, and
     - you do not power on the machine, then configuration update is not applied
     - you power on the machine, then configuration update is applied
   - If the machine is powered on, and
     - you do not restart the machine, then configuration update is not applied
     - you restart the machine, then configuration update is applied

To cancel the configuration update:

You can also cancel a configuration update of a single VM, multiple VMs, or an entire catalog. To cancel a configuration update:

1. Run `Clear-ProvVMUpdateTimeWindow`. For example:
   - To cancel the configuration update scheduled for a single VM:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1”
```

   - To cancel the configuration update scheduled for multiple VMs:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
-VMName "vm1","vm2"
```

NOTE:

The VMs must be from the same catalog.

Change disk encryption

You can change the disk encryption in Azure virtualization environments and do the following:

- Create an MCS machine catalog with disk encryption set (DES) that is different from the master image DES using the `New-ProvScheme` command. For example:

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/
providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/
>

</CustomProperties>

"@

New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName $provisioningSchemeName `

-HostingUnitName $hostingUnitName `

-IdentityPoolName $identityPoolName `

-InitialBatchSizeHint $numberOfVms `

-masterImagePath $masterImagePath `

-NetworkMapping $networkMapping `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-CustomProperties $customProperties
```

- Change the disk encryption type from one DES key to another DES key of an existing MCS machine catalog and existing VMs using `Set-ProvScheme` and `Set-ProvVMUpdateTimeWindow` commands. After you restart the VMs, you can see the updated DES key. For example:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- Update an MCS machine catalog and VM that was not previously CMEK enabled to have customer-managed encryption key (CMEK) encryption (DES), disk encryption at host, or double encryption using `Set-ProvScheme` and `Set-ProvVMUpdateTimeWindow` commands. For information on different encryption types, see Azure server side encryption, Azure disk encryption at host, and Double encryption on managed disk.
- Update an existing MCS machine catalog and VMs to be non-encrypted that was previously encrypted using `Set-ProvScheme` and `Set-ProvVMUpdateTimeWindow` commands. For example:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- Enable disk encryption with private endpoint (an MCS machine catalog that used a host connection enabled with `ProxyHypervisorTrafficThroughConnector`). For more information on `ProxyHypervisorTrafficThroughConnector`, see Create a secure environment for Azure-managed traffic. For information on how to enable disk encryption with private endpoints, see Enable disk encryption with private endpoint.

Enable disk encryption with private endpoint

As per the Azure limitation, currently, you can't have server-side encryption with customer-managed keys for private endpoints. However, you can update an existing MCS machine catalog and VMs with private endpoints to be encrypted with the DES key.

UPDATE AN EXISTING MACHINE CATALOG WITH PRIVATE ENDPOINTS

The detailed steps to update an existing machine catalog with private endpoints are as follows:

1. Create a catalog without disk encryption through `ProxyHypervisorTrafficThroughConnector`. For more information on `ProxyHypervisorTrafficThroughConnector`, see Create a secure environment for Azure-managed traffic.
2. Run `Set-ProvScheme` to update the catalog with `DiskEncryptionSetId`.

   NOTE:

   `DiskEcryptionSetId` can be configured through `CustomProperties` or `MachineProfile`. When it is defined in both `CustomProperties` and `MachineProfile`, the properties defined in `CustomProperties` are applied.

   Example when using `CustomProperties`:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1"/>

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

Example when using MachineProfile: Use a VM that has disk encryption enabled or a template spec with disk encryption settings:

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -MachineProfile
"XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

Alternatively, you can update a machine profile using Studio.

3. Run `Set-ProvVMUpdateTimeWindow` to update existing catalog VMs. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. After you restart the VMs, you can see the updated disk encryption on the VM's disks in Azure portal.
5. Run `Set-ProvScheme` to unset the disk encryption before adding new catalog VMs.

NOTE:

This step is required because you are updating a private endpoint catalog. If you do not do this step, then you get errors while trying to add new VMs to the catalog.

For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

6. Add new VMs to the catalog.

UPDATE INDIVIDUAL CATALOG VMS

The detailed steps to update individual catalog VMs are as follows:

1. Create a catalog without disk encryption through `ProxyHypervisorTrafficThroughConnector`. For more information on `ProxyHypervisorTrafficThroughConnector`, see Create a secure environment for Azure-managed traffic.
2. Run `Set-ProvVM` to update catalog VM with `DiskEncryptionSetId`.

   NOTE:

   The `DiskEcryptionSetId` can be configured through either `CustomProperties` or `MachineProfile`.

   Example when using `CustomProperties`:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-CustomProperties $customProperties
```

Example when using MachineProfile:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

3. Run `Set-ProvVMUpdateTimeWindow` to update existing catalog VMs. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01 -StartsNow -DurationInMinutes -1
```

4. After you restart the VMs, you can see the updated disk encryption on the VMs disks in Azure portal.
5. Add new VMs to the catalog.

Use temporary disk as WBC disk for existing catalogs

You can use Azure temporary disk as write-back cache disk (WBC) disk for existing MCS machine catalogs. Use the `Set-ProvScheme` PowerShell command to update existing catalogs and VMs.

Prerequisites

The existing catalog must satisfy the following conditions:

NOTE:

If the existing catalog doesn't meet the following requirements, the WBC disk is not placed inside the temporary disk.

- MCSIO is enabled: The custom properties `WriteBackCacheMemorySize`, `WriteBackCacheDiskSize`, and `UseWriteBackCache` are enabled.
- Ephemeral OS disk is not enabled.
- WBC is non-persistent: `PersistWBC` is `false`.
- `UseTempDiskForWBC` is null or false.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The temporary disk size must be greater than the total size of (write-back cache disk size + reserved space for paging file + 1 GB buffer space).

IMPORTANT:

Changing a service offering from one with a temporary disk to one without, or the reverse, is not allowed.

Update existing catalogs

To update an existing catalog, run the following commands:

1. Run `Set-ProvScheme` on the existing catalog to update the `UseTempDiskForWBC` to `true`. For example:

```
Set-ProvScheme -ProvisioningSchemeName name -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Standard_LRS`"/><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"ManagedDisksPreview`"
Value=`"False`"/><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"False`"/><Property
xsi:type=`"StringProperty`" Name=`"UseTempDiskForWBC`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"False`"/></CustomProperties>"
```

2. Add new machines to the catalog and power on. The new VMs have a WBC disk inside the temporary disk.

Retrieve information for Azure VMs, snapshots, OS disk, and gallery image definition

You can display information for an Azure VM, including OS disk and type, snapshot and gallery image definition. This information is displayed for resources on the master image when a machine catalog is assigned. Use this functionality to view and select either a Linux or Windows image. A PowerShell property, `TemplateIsWindowsTemplate`, was added to the `AdditionDatafield` parameter. This field contains Azure-specific information: VM type, OS disk, gallery image information, and OS type information. Setting `TemplateIsWindowsTemplate` to **True** indicates

© 1997–2026 Citrix Systems, Inc. All rights reserved.

that the OS type is Windows and setting `TemplateIsWindowsTemplate` to **False** indicates that the OS type is Linux.

TIP:

Information displayed by the `TemplateIsWindowsTemplate` PowerShell property is derived from the Azure API. Sometimes, this field might be empty. For example, a snapshot from a data disk does not contain the `TemplateIsWindowsTemplate` field because the OS type cannot be retrieved from a snapshot.

For example, set the Azure VM `AdditionData` parameter to **True** for Windows OS type using PowerShell:

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

Retrieve region name information for Azure VMs, managed disks, snapshots, Azure VHD, and ARM templates

You can display region name information for an Azure VM, managed disks, snapshots, Azure VHD, and ARM templates. This information is displayed for the resources on the master image when a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

machine catalog is assigned. A PowerShell property called `RegionName` displays the region name information when you run the PowerShell command with the `AdditionalData` parameter.

For example, use the following PowerShell command to get a VM information in Azure.

```
PS C:\Windows\system32> (get-item XDHyp:
\HostingUnits\myAzureNetwork\image.folder\hu-dev-testing-
rg.resourcegroup\hu-dev-tsvda.vm).AdditionalData

Key Value

HardDiskSizeGB 127

ResourceGroupName HU-DEV-TESTING-RG

RegionName East US

TemplateIsWindowsTemplate True

LicenseType

ServiceOfferingDescription Standard_B2ms

ServiceOfferingMemory 8192

ServiceOfferingCores 2

SupportedMachineGenerations Gen1,Gen2

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SecurityType

SecureBootEnabled

VTpmEnabled
```

Clone an MCS catalog

Split an existing persistent and non-persistent MCS catalog into multiple catalogs. By creating a clone of the original provisioning scheme, you can apply different catalog-level policies and configurations to specific subsets of VMs. This functionality is particularly useful when different

© 1997–2026 Citrix Systems, Inc. All rights reserved.

functional roles within an organization, such as Finance or Executives, require different resource configurations (for example, backup limits) compared to standard users.

Example usage

An administrator manages a large catalog of VMs. The Executive team requires a higher number of backups than the standard policy allows. The administrator uses the `Copy-ProvScheme` command to clone the existing catalog provisioning scheme into a new catalog. This allows the administrator to apply a dedicated backup policy to the new Executive catalog while maintaining the original settings for the rest of the organization.

Applicability

- Azure environments
- Persistent and non-persistent MCS catalogs
- MCS provisioned Citrix Provisioning catalogs

Limitations

- **Provisioning scheme:** Only the latest version of the provisioning scheme is copied.
- **Backup schedules**: The backup schedule is not copied to the new catalog; the new catalog must have its own backup schedule configured.
- **Identity pools**: Identity-related objects are not cloned and remain shared using the same `ADAccountIdentityPool`.
- **Delivery groups**: Delivery group operations and user assignments are not changed or associated during the cloning process.

Important considerations

- **Resource Groups (TargetLocation)**:
  - If you do not provide a `TargetLocation` (Azure Resource Group):
    - For a Citrix managed resource group, a new Citrix managed resource group is created.
    - For a BYO (Bring Your Own) resource group, the new provisioning scheme resources are created in the same resource group.
  - If you provide a `TargetLocation`:
    - The resources are created in the provided resource group.
    - The specified resource group must already exist in Azure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Base Disk Snapshot**: A copy of the base disk snapshot is always made, regardless of the resource group configuration.

Prerequisites

- An existing provisioning scheme (source catalog) must be available.
- If specifying a target location, the target Azure Resource Group must exist.

Configure using PowerShell

1. Open a PowerShell window.
2. Run the `Copy-ProvScheme` command using the required parameters: `SourceProvisioningSchemeName` (or `SourceProvisioningSchemeUid`) and `TargetProvisioningSchemeName`.

   Example 1: Copy a provisioning scheme by name.

   This example copies the scheme named "Backup" to a new scheme named "TestCopy".

   ```
   Copy-ProvScheme -SourceProvisioningSchemeName Backup
   -TargetProvisioningSchemeName TestCopy
   ```

   Example 2: Copy a provisioning scheme by Uid to a specific Resource Group

   This example copies a scheme using its Uid and specifies a target resource group named "TestRg".

   ```
   Copy-ProvScheme -SourceProvisioningSchemeUid 771e205d-1ee5-4ad2-b044-
   ecf3d7f24ec7 -TargetProvisioningSchemeName TestCopy -TargetLocation
   TestRg
   ```

Identify resources created by MCS

Following are the tags that MCS adds to the resources on Azure platform. The tags in the table are represented as "key":"value".

RESOURCE NAME	TAG
ID disk	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE NAME	TAG
Image	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
NIC	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
OS disk	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
Preparation VM	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
Published snapshot	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
Resource group	"CitrixResource" : "Internal"
	CitrixSchemaVersion: 2.0
	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Storage account	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
VM in catalog	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE NAME	TAG
WBC disk	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"

NOTE:

A VM is not visible in the Citrix inventory if a **CitrixResource** tag is added to identify it as a resource created by MCS. You can remove or rename the tag to make it visible.

Remove tags

When you create a catalog or a VM, tags are created on the following resources:

- Resource group
- Virtual machine
- OS disk
- Identity disk
- Network interface
- Storage account

You can remove VMs and machine catalogs from the Citrix database and remove tags. You can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and tags from a single VM or a list of VMs from a machine catalog.
- `Remove-ProvScheme` with `ForgetVM` parameter to remove a machine catalog from the Citrix database and tags from an entire machine catalog.

This feature is only applicable to persistent VMs.

To do this:

1. Open a **PowerShell** window.
2. Run **asnp citrix*** to load the Citrix-specific PowerShell modules.
3. Run `Remove-ProvVM` to delete VMs from Citrix database and tags from VMs. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName
“vmname” -ForgetVM
```

4. Run `Remove-ProvScheme` to delete machine catalog from Citrix database and tags from machine catalogs. For example:

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName”
-ForgetVM
```

NOTE:

After you use `ForgetVM` parameter in `Remove-ProvScheme`, MCS deletes all snapshots including base disk snapshot if the provisioning scheme is present in either bring your own resource group (BYORG) or Citrix managed resource group.

More information

- Create and manage connections and resources
- Connection to Microsoft Azure
- Create machine catalogs
- Create a Microsoft Azure catalog
- Manage machine catalogs

Manage a Microsoft SCVMM catalog

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to Microsoft System Center Virtual Machine Manager (VMM) virtualization environments.

NOTE:

Before managing a VMM catalog, you need to finish creating a VMM catalog. See Create a Microsoft System Center Virtual Machine Manager catalog.

Identify resources created by MCS

Following are the tags that MCS adds to the resources on SCVMM platform. The tags in the table are represented as "key":"value".

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE NAME	TAG
Preparation VM	Tag string: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	Custom property entry: "XdConfig:"XdProvisioned=True"
VM in catalog	Tag string: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	Custom property entry: "XdConfig:"XdProvisioned=True"

More information

- Create and manage connections and resources
- Connection to Microsoft System Center Virtual Machine Manager
- Create machine catalogs
- Create a Microsoft System Center Virtual Machine Manager catalog
- Manage machine catalogs

Manage a Nutanix catalog

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to Nutanix AHV Prism Central environments.

NOTE:

Before managing a machine catalog on Nutanix AHV Prism Central, you need to finish creating a machine catalog on Nutanix AHV Prism Central. See Create a Nutanix catalog.

You can manage a machine catalog on Nutanix AHV Prism Central using:

- Studio
- PowerShell

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use Studio

Following are the options to manage a machine catalog on Nutanix AHV Prism Central using Studio:

OPTION	DESCRIPTION
Add Machines	Create and add VMs to the machine catalog.
Delete Machine Catalog	Delete a machine catalog. You can choose to delete VMs at the same time or leave persistent VMs intact.
Change Master Image	Change the master image used as a template for all VMs in the catalog.
Add or change Machine Profile	Change the template version of the machine profile or add a machine profile to an existing catalog.
Manage Configuration Set	Bind a catalog to a Workspace Environment Management™ configuration set or switch to a different configuration.
Edit Machine Catalog	Modify configurations for the catalog, such as NICs and Virtual Machines.
View Machines	Jump to the **Search** node to see all VMs that belong to the catalog.
Rename Machine Catalog	Change the catalog name.
Upgrade VDAs	Upgrade VDAs on a per-catalog basis. This feature only applies to static persistent machines.
Change Functional Level	Select the minimum functional level for the catalog. Setting a functional level makes all features available.
Test Machine Catalog	Test whether the catalog has errors or warnings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTION	DESCRIPTION
Manage Tags	Create, edit, and delete tags. Select tags to apply to the catalog.
Move Machine Catalog	Move the catalog to another folder.

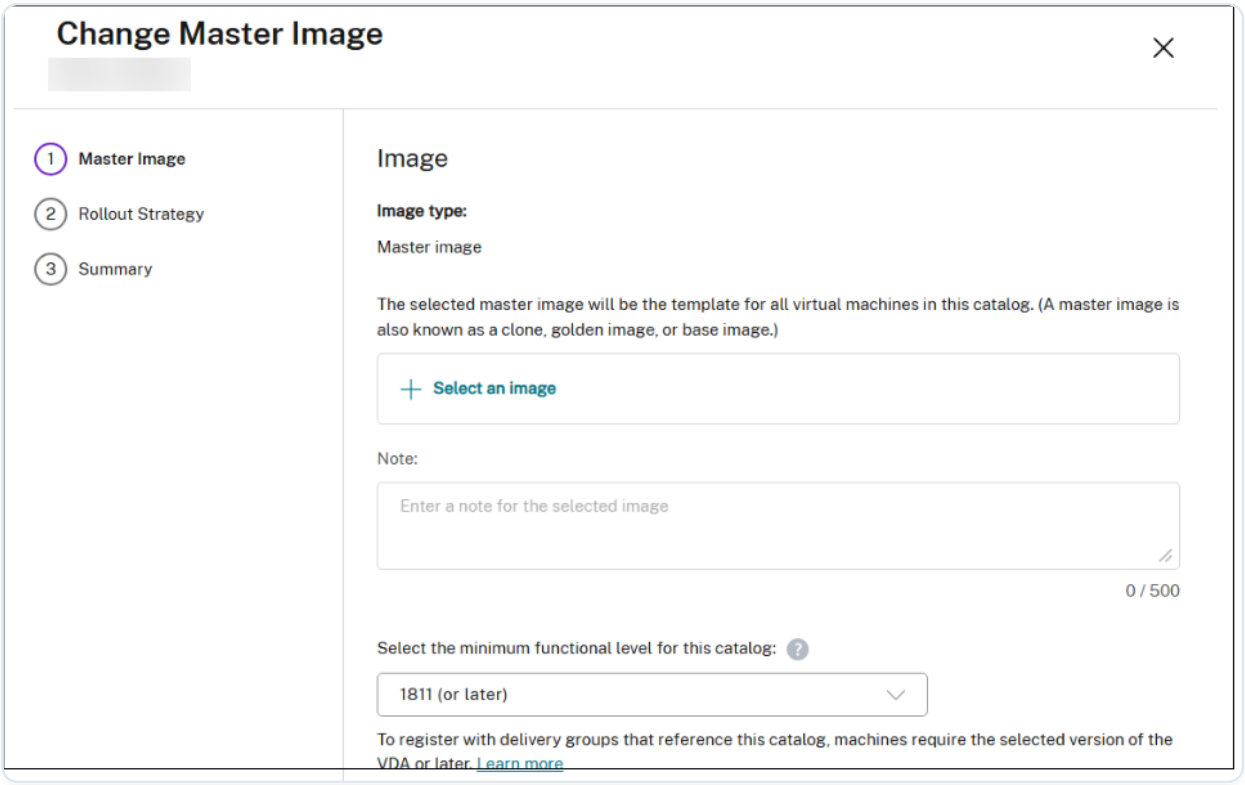
NOTE:

Currently, the **Clone** option is not available.

Change master image

To change the master image for a catalog, follow these steps:

1. On the **Machine Catalogs** page, right-click the machine catalog you want to update, and select **Change Master Image**.
2. On the **Change Master Image** page, click **Select an image**.



3. On the **Select an image** page, expand a template and select a template version to use as the master image. You can filter machine templates by name.
4. On the **Rollout Strategy** page, choose when you want the update to be applied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- For an MCS provisioned non-persistent catalog with the Nutanix AHV Prism Central host connection plug-in, updating the master image to switch the boot configuration between Legacy and UEFI, prevents existing VMs from starting at their next boot.
- When you update the master image, only the OS disk is update. The hardware properties remain unchanged. To update the hardware properties, see Add or change the machine profile, Change NICs and Change VMs configuration.

Add or change the machine profile

To add or change a machine profile for a catalog, follow these steps:

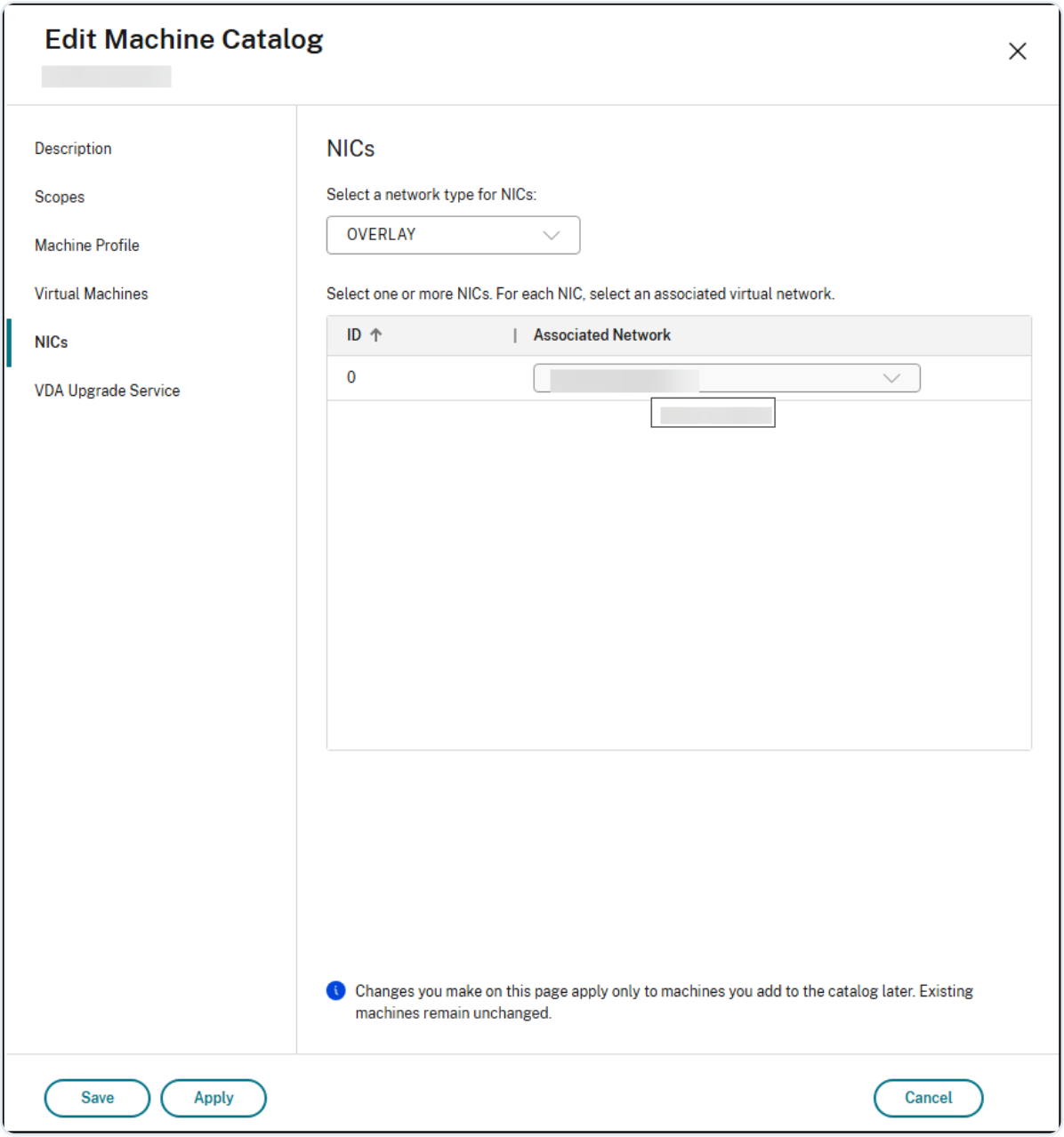
1. On the **Machine Catalogs** page, right-click the machine catalog you want to modify, and select **Edit Machine Catalog**.
2. On the **Machine Profile** page,
   - If the machine catalog already has a machine profile, then click the pencil icon to select a different machine profile template version. You can filter by the template name. Confirm the machine profile settings.
   - If the machine catalog doesn't have a machine profile, then select Use a machine profile and select a machine profile. Confirm the machine profile settings.
3. The **Virtual Machines** page must reflect the updated configuration as per the selected machine profile template version.

Change NICs

To change NICs for a catalog, follow these steps:

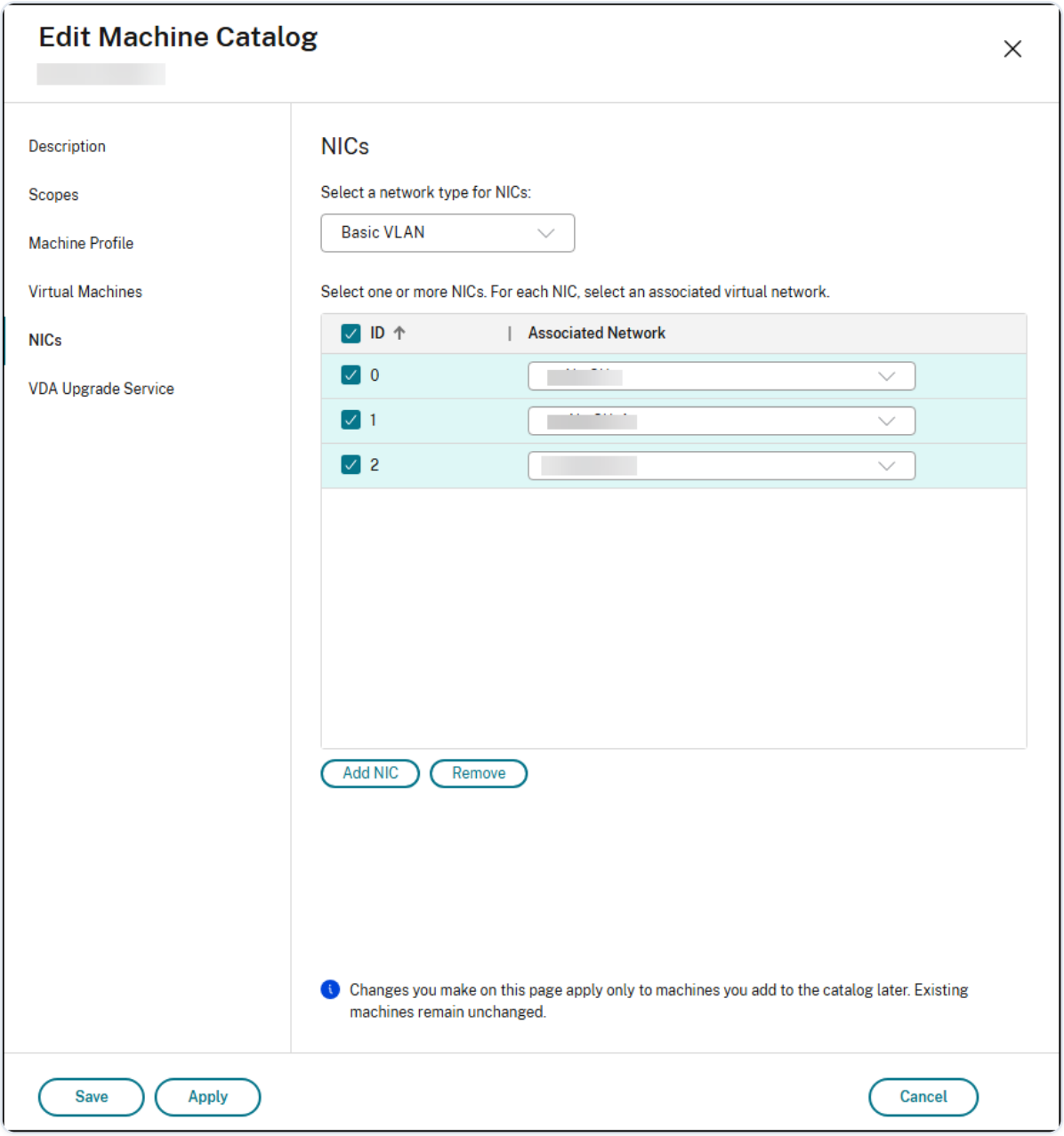
1. On the **Machine Catalogs** page, right-click the machine catalog you want to modify, and select **Edit Machine Catalog**.
2. On the **NICs** page:
   - Select a **NIC** type.
   - If the selected catalog was created with a machine profile, then the NIC number is consistent with the NIC number of machine profile and can't be changed. Select an associated virtual network for each NIC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- If the selected catalog was created without machine profile, click **Add NIC** to increase NIC count or click **Remove** to delete selected NICs. Select or clear the boxes to select NICs, and choose an associated virtual network for each NIC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

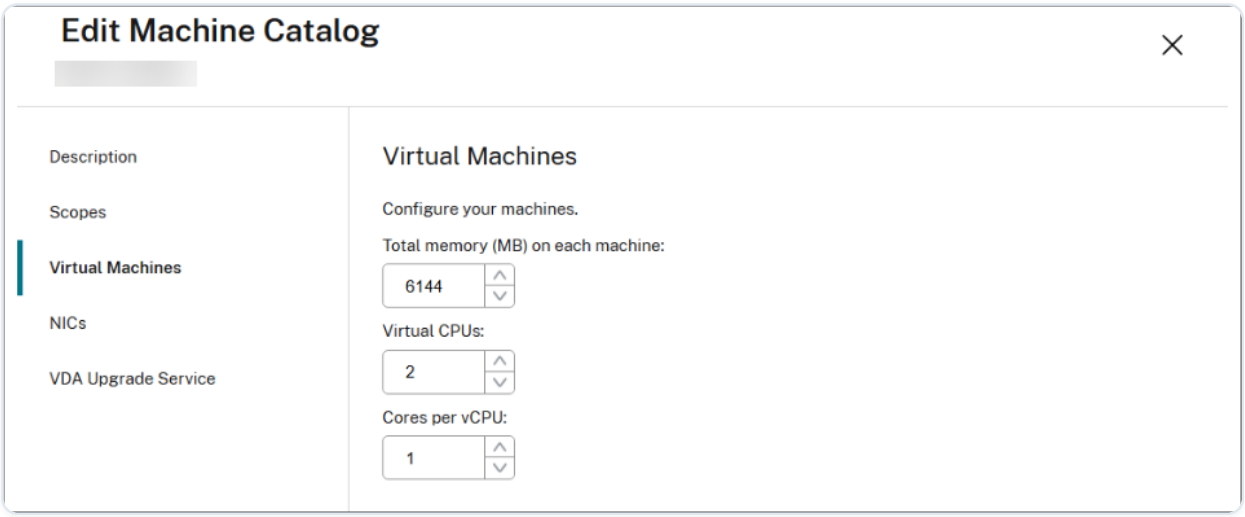


Change VMs configuration

To change the configuration of VMs, including Memory, CPU count, and Cores per vCPU, follow these steps:

1. On the **Machine Catalogs** page, right-click the machine catalog you want to modify, and select **Edit Machine Catalog**.
2. On the **Virtual Machines** page, use the up or down arrow, or enter values directly to adjust the Memory, CPU count, and Cores per vCPU for the VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Use PowerShell

Change master image

The required parameters are:

- `ProvisioningSchemeName`: Name of the provisioning scheme to edit.
- `MasterImage`: Literal path to the new master image.

Run the following command. For example:

```
Set-ProvSchemeMetadata  -Name "ImageManagementPrep_DoImagePreparation"
-ProvisioningSchemeName "<ProvisioningSchemeName>" -Value "True"



Publish-ProvMasterVMImage  -MasterImageVM "<Literal path to the new master
image- template version> -ProvisioningSchemeName
"<ProvisioningSchemeName>" -RunAsynchronously
```

NOTE:

When you update the master image, only the OS disk is update. The hardware properties remain unchanged. To update the hardware properties, see Add or change the machine profile, Change NICs and Change NIC and VM's configuration.

Add or change machine profile

Use the `Set-ProvScheme` command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To update a catalog with a new machine profile, or
- To update an existing catalog that does not have a machine profile to start using the machine profile as the source of hardware specification.

NOTE:

This does not update the hardware specification of the existing VMs in the catalog. Only the new VMs added to the catalog have the hardware specification from the given machine profile.

To change machine profile or convert an existing catalog to start using machine profile:

```
Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `


               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion"

               -NetworkMapping @{"0"="XDHyp:\HostingUnits\<Hosting unit
name>\Clusters.folder\<Cluster Name>.cluster\<Network name>.network"}
```

The machine profile must have at least one NIC, and the number of NICs in the machine profile must match the subnet mappings in NetworkMapping

The total number of NICs for the template version can be obtained from the `AdditionalData` of its inventory item using the following:

```
$tv = Get-Item -Path "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion"

$tv.AdditionalData.TotalNics
```

To change machine profile with overridden hardware specification:

Certain configurations can be configured using specific command-line parameters. These command line parameters, such as `VMCpuCount` and `VMMemoryMB`, and `CPUCores` in the `CustomProperties`, takes precedence over the values in the Machine Profile template version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$customProperties = @"

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

        <StringProperty Name="CPUCores" Value="2" />

    </CustomProperties>

"@



Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `

               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion" `

               -CustomProperties $customProperties `

               -VMCpuCount 4 `

               -VMMemoryMB 4096
```

Change NIC and VM's configuration

The required parameters are:

- `ProvisioningSchemeName`: Name of the provisioning scheme to edit.
- `NetworkMapping`: Updated network mapping.

Run the following command. For example:

```
Set-ProvScheme  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"ClusterId`" Value=`"000xxxx-1fb0-xxxxx-4fc8-5c257335xxxx`" /
><Property xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>"  -NetworkMapping @{"6"="XDHyp:\HostingUnits\<Hosting
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Unit Name>\Clusters.folder\<Cluster Name>\<Network name>.network"}
-ProvisioningSchemeName "<ProvisioningSchemeName>" -VMCpuCount 4
```

Reset OS disk for persistent VMs

Resetting the OS disk in persistent VMs, especially those with vTPM enabled, can break applications relying on vTPM keys and BitLocker, potentially preventing boot. Therfore, this feature allows:

- Resetting the OS disk for persistent VMs and preserving VM hardware configurations.
- Managing vTPM-enabled VMs to avoid breaking vTPM dependency during disk swaps.

You can reset OS disk for persistent VMs using the `Reset-ProvVMDisk` PowerShell command.

- For vTPM-enabled VMs: A new VM is created from a recovery point using the original hardware info, preserving vTPM keys.
- For non-vTPM VMs: The OS disk is replaced.

For examples, see Reset OS disk.

Migrate machine catalogs to Citrix-managed Nutanix AHV Prism Central host connection

Migrate your Citrix machine catalogs, and their associated VMs from existing Nutanix AHV (for Prism Element) and Nutanix AHV PC (for NC2 on Azure) host connections to the Citrix-managed Nutanix AHV Prism Central host connection. For migration, use PowerShell commands, which also include fast rollback options in case of issues, and commands to clean up source resources post-migration.

Benefits

- **Minimized disruption**: You smoothly transition to the Nutanix AHV Prism Central plug-in. This has minimal impact on your existing deployments.
- **Seamless upgrade path**: It provides a clear, and supported path for you to upgrade your infrastructure, and leverage the new management interface.
- **Data integrity and safety**: Rollback options ensure you revert the environment to its original state in case of unforeseen issues. This reduces risk.
- **Resource efficiency**: You clean up source resources after successful migration. This optimizes storage, and management overhead.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Flexibility**: It supports migration for catalogs provisioned by both MCS, and third-party technologies. This offers broader applicability.

Applicability

This feature is applicable to machine catalogs under Nutanix AHV (for Prism Element) and Nutanix AHV PC (for NC2 on Azure) host connections:

- Machine catalogs managed by MCS, including both persistent and non-persistent types.
- Power-managed-only machine catalogs that contain VMs provisioned by third-party technologies.

System Requirements

- **Nutanix AHV Prism Element (PE) AOS Version**: You require a minimum of 6.8.
- **Nutanix Prism Central (PC) Version**: You require a minimum of 2024.3.

NOTE:

Nutanix Prism Central 7.3 requires AOS 7.3 due to a Nutanix known issue.

Limitations

- **PVS catalogs arent supported**: This feature **doesn't** support machine catalogs created using **Citrix Provisioning Services** (PVS) Xendesktop Setup Wizard.
- **Rollback restrictions**:
  - Only allow rollback of a migrated catalog if you **haven't** modified the catalog after the initial migration.
  - When you execute the "**Cleanup Source Resources**" operation, it clears the migration state. This prevents any subsequent rollback.
- **No re-migration**: A machine catalog that you already migrated isn't supported for re-migration.
- **Multi-host connection VMs**: Migration of power-managed-only machine catalog that contains VMs imported from multiple host connections is not supported.

Important Considerations

- **Nutanix cluster management**: Hosting Nutanix AHV clusters must be registered to a Nutanix Prism Central. .

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Master image template creation**: For MCS machine catalogs, the migration command provides an option to generate a vm template version on Prism Central from the original snapshot of the machine catalog master image. This vm template version can later be used as the MCS master image of machine catalogs under Prism Central host connection. By default, this option is not enabled.
- **Rollback pre-conditions**:

  For a successful rollback to be possible, the original source environment—including the host connection, base disks—must remain unchanged. You must also avoid making any configuration changes to the migrated machine catalog and adding/removing VMs until the migration is confirmed to be successful. After that confirmation, you may perform the final Cleanup Source Resources operation, but be aware that this is an irreversible step that will make a rollback impossible.

Required permissions for migration and rollback

To migrate catalogs or rollback, you need the following permissions:

Prism Element administrator:

- Create Virtual Machine

Prism Central administrator:

- Create VM Templates
- Delete VM Templates
- Delete VM Recovery Point
- Delete Virtual machine

For the complete list of specific permissions needed for Citrix-managed Nutanix AHV Prism Central host connection, see Required permissions.

How to migrate

You manage this feature through dedicated PowerShell cmdlets. The general workflow involves three main operations: Migration, Rollback, and Cleanup source resources.

Migrate a machine catalog

- This operation moves a machine catalog, and its associated VMs from a source Nutanix AHV or Nutanix AHV PC host connection to a target Citrix-managed Nutanix AHV Prism Central host connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For MCS provisioned catalogs, this process creates new base disks in the target connection .
- You optionally choose to create a master VM equivalent (VM template version) in the target connection from the original master image snapshot.

1. **Create a new Nutanix AHV Prism Central host connection**: Before migrating, register the hosting Nutanix AHV cluster to a Nutanix Prism Central, and establish a new Nutanix AHV Prism Central host connection that points to the target Nutanix Prism Central instance. This connection serves as the destination for your migrated catalogs. For details, see Nutanix AHV Prism Central host connection.
2. **Migrate an existing machine catalog**: For an existing machine catalogs, use the `Switch-ProvCatalog` PowerShell cmdlet to initiate the migration to Citrix-managed Nutanix AHV Prism Central host connection.

   ```
   c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID>
   -DestinationHypervisorConnectionName "DestinationConnection"
   -DestinationHostingUnitName "DestinationUnit"
   -CreateMasterImageAtDestination
   ```

   - Replace `<Catalog_UID>` with the unique identifier of the machine catalog you wish to migrate. Use following PowerShell cmdlet to locate the `BrokerCatalogUid` by catalog name `Get-BrokerCatalog -Name <Catalog Name>`.
   - `DestinationConnection` is the name of the new **Nutanix AHV Prism Central host connection** created in Step 1.
   - `DestinationUnit` is the name you give to the hosting unit within the `DestinationConnection` where the machine catalog will reside.
   - The `-CreateMasterImageAtDestination` parameter is optional. It creates a master image VM template version on the target Prism Central.
3. **Verify migration completion**: After executing the migration cmdlet, monitor the task status in the PowerShell window to ensure it completes successfully. When the migration completes, the catalog is moved to the target host connection created in step 1. You must see a status finished with the task type SwitchProvCatalog. Followings are recommended steps to verify the migration completion:

   - Check the status of the catalog in Studio.
   - Verify that the VMs within the catalog are now associated with the new destination hypervisor connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Verify that the VMs within the catalog are showing the correct power state.
- Test the functionality of the migrated machine catalog by adding or removing machines or issuing power operations ensuring that the catalog is functioning correctly.

Rollback a migrated catalog

This operation reverts a machine catalog, and its VMs to their original source host connection. It removes any resources you created during the migration process.

IMPORTANT:

You only perform rollback if you have not modified the catalog after migration, and you have not run the **Cleanup Source Resources** operation. The original source connection remains unchanged, and still contains its base disks.

```
c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID> -Rollback
```

Clean up source resources

After a successful migration, this operation removes source resources, for example, base disks, from the original hypervisor connection.

IMPORTANT:

When you execute this command, it clears the migration state. This makes subsequent rollbacks impossible.

```
c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID>
-CleanupSourceResources
```

You receive a confirmation prompt before proceeding, as this action is irreversible. Acknowledge the prompt to complete the cleanup.

More information

- Create and manage connections and resources
- Connection to Nutanix
- Connection to Nutanix cloud and partner solutions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Create machine catalogs
- Create a Nutanix catalog
- Manage machine catalogs

Manage a VMware catalog

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to VMware virtualization environments.

NOTE:

Before managing a VMware catalog, you need to finish creating a VMware catalog. See Create a VMware catalog.

Update provisioned VMs to current provisioning scheme state

The `Set-ProvScheme` command changes the provisioning scheme. However, it does not affect existing VMs. Using the PowerShell command `Set-ProvVMUpdateTimeWindow`, you can apply the current provisioning scheme to an existing persistent or non-persistent VM or set of VMs. This feature is applicable to machine profile and non-machine profile-based machine catalog.

You can update the following:

- VMCpuCount: Provisioning scheme property
- VMMemoryMB: Provisioning scheme property
- Folder ID: Custom property
- Subnet mapping: Provisioning scheme property
- Hardware version of VM: Only for machine profile-based machine catalog
- Machine profile: Only for machine profile-based machine catalog

You can update:

- A single VM
- A list of specific VMs or all existing VMs associated with a provisioning scheme ID
- A list of specific VMs or all existing VMs associated with a provisioning scheme name (machine catalog name)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Before updating the existing VMs

1. Check the configuration of the existing VMs. For example:

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. Update the provisioning scheme. For example:

```
$customProperties=<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="FolderId"
Value="FOLDER_ID"/></CustomProperties>

$memoryMb=<DOUBLE THE "UPDATE" MACHINE PROFILE>

Set-ProvScheme -ProvisioningSchemeName my-catalog -VMCpuCount 4
-VmMemoryMb $memoryMb -CustomProperties $customerProperties
-NetworkMapping @{"1" = "<A_NETWORK_PATH_FROM_THE_HOSTING_UNIT>"}
-MachineProfile "<PATH_TO_UPDATE_MACHINE_PROFILE>"
```

3. Check if the current property of the VM matches the current provisioning scheme, and if there is any pending update action on the VM. For example:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

   You can also find VMs with a particular version. For example:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

Request updates for existing VMs to apply at the next restart

1. Run the following commands to update existing VMs and have the updates apply at the next restart.

   - To update all the existing VMs. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

- To update a list of specific VMs. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

- To update VMs based on the output of `Get-ProvVM`. For example:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

NOTE:

- The `StartsNow` indicates that the scheduled start time is the current time.
- The `DurationInMinutes` with a negative number (for example, –1) indicates no upper bound on the schedule's time window.

2. Find VMs with an update scheduled. For example:

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. Restart the VMs. At the next power-up, property changes are applied to the existing VMs. You can check the updated status using the following command. For example:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Cancel the configuration update

You can also cancel a configuration update of a single VM, multiple VMs, or an entire catalog. To cancel a configuration update:

1. Run `Clear-ProvVMUpdateTimeWindow`. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To cancel the configuration update scheduled for a single VM:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1”
```

- To cancel the configuration update scheduled for multiple VMs:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
-VMName "vm1","vm2"
```

NOTE:

The VMs must be from the same catalog.

Update the folder ID of a machine catalog

You can update the folder ID of an MCS machine catalog by specifying the `FolderId` in the custom properties of `Set-ProvScheme` command. The VMs created after updating the folder ID are created under this new folder ID. If this property is not specified in `CustomProperties`, then VMs are created under the folder where the master image is located.

Perform the following steps to update the folder ID of a machine catalog.

1. Open a Web browser and enter the URL for the **vSphere Web Client**.
2. Enter the credentials and click **Login**.
3. Create a VM placement folder in **vSphere Web Client**.
4. Open a PowerShell window.
5. Run **asnp citrix®*** to load the Citrix-specific PowerShell modules.
6. Specify the `FolderID` in the `CustomProperties` of `Set-ProvScheme`. In this example, the folder ID value is `group-v2406`.

```
Set-ProvScheme -ProvisioningSchemeUid
"50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
"<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
Value=""group-v2406"" /></CustomProperties>"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Add a VM to the machine catalog using Studio.
8. Check the new VM on vSphere Web Client. The new VM is created under the new folder.

Find the folder ID using PowerShell commands

Use the PowerShell command `Get-HypConfigurationDataForItem` to find the folder ID for an existing folder in a VMware Hypervisor.

Create a hosting connection and resource group for a VMware Hypervisor. Then, perform the following steps to find the folder ID of a folder on that hypervisor.

1. Determine the `XDHyp` path to the root of the VM folder tree. For example:

   ```
   XDHyp:\Connections\VMwareConn\Datacenter.datacenter
   ```

2. Use `Get-HypConfigurationDataForItem` to retrieve the tree structure. For example:

   ```
   Get-HypConfigurationDataForItem -LiteralPath XDHyp:
   \Connections\VMwareConn\Datacenter.datacenter
   ```

3. Run the following command to identify the folder ID from the output XML. In this example, look for the folder ID of `ExampleFolder` in the XML output.

   ```
   $result = Get-HypConfigurationDataForItem -LiteralPath XDHyp:
   \Connections\VMwareConn\Datacenter.datacenter

   $result.VmPlacementFolder
   ```

   XML output:

   ```
   <?xml version="1.0" encoding="utf-16"?>

   <CtxVmPlacementFolder xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

   <Name>vm</Name>

   <Id>group-v4</Id>

   <SubFolder>
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<CtxVmPlacementFolder>
  <Name>vCLS</Name>
  <Id>group-v75</Id>
  <SubFolder />
</CtxVmPlacementFolder>
<CtxVmPlacementFolder>
  <Name>MyOtherFolder</Name>
  <Id>group-v1110</Id>
  <SubFolder />
</CtxVmPlacementFolder>
<CtxVmPlacementFolder>
  <Name>ExampleFolder</Name>
  <Id>group-v4658</Id>
  <SubFolder />
</CtxVmPlacementFolder>
</SubFolder>
</CtxVmPlacementFolder>
```

Find the folder ID in vSphere

Access the MOB on any ESXi or vCenter server system to find the folder ID of the VMs.

The Managed Object Browser (MOB) is a web-based server application available inbuilt in all ESX/ESXi and vCenter server systems. This vSphere utility allows you to view detailed information about objects like VMs, datastores, and resource pools.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open a web browser and enter `http://x.x.x.x/mob`, where x.x.x.x is the IP address of the vCenter Server or ESX/ESXi host. For example, `<https://10.60.4.70/mob>`.
2. On the **Home** page of MOB, click the value of the property **content**.
3. Click the value of the **rootFolder**.
4. Click the value of the **childEntity**.
5. Click the value of the **vmFolder**.
6. You can find the folder ID in the value of the **childEntity**.

Identify resources created by MCS

Following are the tags that MCS adds to the resources on VMware platform. The tags in the table are represented as "key":"value".

RESOURCE NAME	TAG
Preparation VM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"
VM in catalog	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"

More information

- Create and manage connections and resources
- Connection to VMware
- Create machine catalogs
- Create a VMware catalog
- Manage machine catalogs

Manage a XenServer® catalog

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to XenServer virtualization environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Before managing a XenServer catalog, you need to finish creating a XenServer catalog. See Create a XenServer catalog.

Identify resources created by MCS

When the Machine Creation Services™ (MCS) generates resources like disks, it assigns a ProvisioningScheme ID tag for better utilization of those resources.

Tags are helpful to administrators as they can better manage and organize the resources. For example, if resources, like unused disks, are tagged, then administrators can easily identify where the resource is created, making the cleanup process efficient.

Following are the tags that MCS adds to the resources on XenServer platform. The tags in the table are represented as "key":"value".

RESOURCE NAME	TAG
Copy of disk on each network or local storage (on-prem only)	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ID disk	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OS disk	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Preparation VM	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM in catalog	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
WBC disk	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Retrieve information about provisioning scheme

To retrieve detailed information about the provisioning scheme, you can execute the following PowerShell commands. Replace `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx` with the actual Provisioning Scheme ID:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Replace the placeholder ID with your actual Provisioning Scheme ID

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

2. Retrieve detailed information about the provisioning scheme:

```
Get-ProvisioningScheme -Id $provisioningSchemeId
```

Retrieve list of resources created by MCS

Run the following commnds to get a comprehensive list of resources created by MCS.

1. Replace the placeholder ID with your actual Provisioning Scheme ID.

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

2. Retrieve the entire list of resources created by MCS.

```
Get-ProvResource -ProvisioningSchemeUid $provisioningSchemeId |
ConvertTo-JSON -Depth 6
```

After execution, you get the following output:

- The name and ID of the provisioning scheme.
- A list of provisioning image versions within the provisioning scheme. Each entry includes:
  - The image name and ID.
  - The Disk ID and Storage ID of the disk.
- A list of provisioning VMs. Each entry includes:
  - The OS disk ID and parent disk ID of the OS disk .
  - The Storage ID of the OS disk.
  - The Identity disk and its Storage ID.

More information

- Create and manage connections and resources
- Connection to XenServer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Create machine catalogs
- Create a XenServer catalog
- Manage machine catalogs

Power Management

With Citrix DaaS™, you can power manage MCS-provisioned VMs across various supported hypervisors and cloud services. The power management operation provides you:

- Optimal user experience
- Cost management and power savings

The power actions available are:

- Start
- Shut down
- Restart
- Suspend
- Resume
- Force restart
- Force shutdown

NOTE:

- For a non-persistent VM, power cycle (shutdown/start and restart) results in OS disk getting reset.
- Power action capabilities and behaviors vary depending on hypervisors or cloud services.

The article covers key power management features associated with certain supported hypervisors.

- Power manage Amulet Hotkey CoreStation VMs
- Power manage AWS VMs
- Power manage Azure VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Power manage Amulet Hotkey CoreStation VMs

Citrix DaaS™ lets you do power management of Amulet Hotkey CoreStation VMs. Use the **Search** node in the navigation pane to locate the machine you want to power manage.

The following power actions are available:

- Start
- Shut Down
- Force Shutdown
- Force Restart
- Restart

NOTE:

- Reset, Suspend, and Resume power actions are not supported.
- Shut Down/Restart: Request the node to Shutdown the operating system and turn off. This is equivalent to a short press on the power button for a physical desktop machine. The Workstation might not respond to the shutdown request if there are active users or running programs which interrupt the shutdown or OS updates need to be installed.

More information

- Amulet Hotkey CoreStation virtualization environments
- Connection to Amulet Hotkey CoreStation
- Create an Amulet Hotkey CoreStation machine catalog

Power manage AWS VMs

For information on required permissions, see About AWS permissions.

AWS on-demand provisioning

With this on-demand provisioning, the OS disk gets deleted when you shut down a non-persistent VM. After you power on the VM, a new VM is created from the master image which has an OS disk and ID disk. To determine if a VM has on-demand feature enabled or not, run `Get-ProvVM` PowerShell command. If the property `CustomVMData` has all VM specific values, implies that the VM has on-demand feature enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instance Hibernation

The hibernation process stores the in-memory state of the instance, along with its private, and elastic IP addresses, allowing it to pick up exactly where it left off.

When an instance is instructed to hibernate, it writes the in-memory state to a file in the root EBS volume, and then shuts itself down. An Amazon EBS volume is a durable, block-level storage device that you can attach to your instances. After you attach a volume to an instance, you can use it as you would use a physical hard drive. Encrypt the root EBS volume of the instance. The encryption ensures proper protection for sensitive data when it is copied from memory to the EBS volume. For information on EBS encryption, see Amazon EBS encryption.

Following are the limitations of the supported instance hibernation:

- Instance memory (RAM) of only up to 150 GB is supported
- UEFI boot mode is not supported
- The General Purpose SSD and Provisioned IOPS SSD are only supported as EBS volume types.

Create hibernation supported VMs

To create hibernation supported VMs:

1. Create a host connection. See Connection to AWS.
2. Launch an instance with EBS root encrypted and the **Stop-Hibernate** property enabled. For more information, see:
    - Instance lifecycle
    - Amazon EBS encryption
    - Hibernation prerequisites
    - Enable hibernation for an instance
    - Hibernate your On-Demand Instance or Spot Instance
3. Use this instance as a master image to create an AMI.
4. Prepare the master image:
    a. Install a VDA on the master image. Citrix recommends installing the latest version to allow access to the newest features. Failure to install a VDA on the master image causes the catalog creation to fail. For more information on how to install a VDA, see Install VDAs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Join the master image to the domain where applications and desktops are members. Ensure that the master image is available on the host where the machines are created.

5. Create an AMI from that instance. For information on creating an AMI from an instance, see Create an AMI from an Amazon EC2 Instance.
6. Create a machine catalog using `New-ProvScheme` command. Set the `AwsCaptureInstanceProperties` custom property as **True**.

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

-CustomProperties "AwsCaptureInstanceProperties,true;"

-HostingUnitName "xxx" -IdentityPoolName $catalog_name
-InitialBatchSizeHint 1

-MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
(vpc-0f1771e45671aedcd).network"}

-ProvisioningSchemeName $catalog_name

-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
"xxx"
```

For information on creating machine catalog using PowerShell commands, see `<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>`.

VMs that can be hibernated are created if:

- You select an AMI created from a master image that has the **Stop-Hibernate** property enabled.
- The master VM is domain joined and has the VDA installed.
- You select the correct VM size (service offering) that can handle hibernation.

The **New-ProvScheme** command fails with an appropriate error message if:

- The master VM is hibernation enabled but the service offering is not capable of handling hibernation.
- If the master VM is not domain joined and has no VDA installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hibernation status of service offerings and AMI

To get the hibernation status of the service offerings and AMI (templates), run the following commands:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

Update service offering of an existing hibernation supported provisioning scheme

1. Run the `Set-ProvScheme` command. For example,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

The system displays an exception message if the service offering is not compatible.

Create machine catalog with hibernation support

When creating machine catalogs, you can use a machine profile that supports hibernation.

1. In the catalog creation wizard, follow the instructions till the selection of the machine profile.
2. On the **Machine Template** page, click **Select a machine profile** and select a machine profile.
3. On the **Virtual Machine** page, click the **Edit** icon and select a VM.

> **NOTE:**
>
> If the machine profile is hibernation enabled, the system displays only those VMs that can be hibernated.

4. Follow the onscreen instructions to complete all settings. The **Summary** page displays the hibernation status of the catalog.

> **NOTE:**
>
> In the edit machine catalog, when you change the machine profile to a hibernation-enabled one, you are be asked to reconfigure your VMs accordingly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Update machine catalog that supports hibernation

If you try to update an existing machine catalog with a machine catalog that does not support hibernation, the update fails with an appropriate error message.

Power management of hibernated VMs

You can do the following power management operations on the hibernated VMs:

1. Suspend the VM from the running state.
2. Resume VM from the suspended state.
3. Restart VM from the suspended state.

To see the power management options, in Studio, right-click the hibernated VMs.

You can also see the power state as **Suspending** and **Suspended** for each VM as per the power operations you perform on the VMs.

Power manage Azure VMs

For information on required permissions, see Required Azure permissions.

Azure on-demand provisioning

With Azure on-demand provisioning, VMs are created only when Citrix DaaS™ initiates a power-on action, after the provisioning completes.

When you use MCS to create machine catalogs in the Azure Resource Manager, the Azure on-demand provisioning feature:

- Reduces your storage costs
- Provides faster catalog creation

When you create an MCS catalog, the Azure portal displays the network security groups, network interfaces, base images, and identity disks in the resource groups.

The Azure portal does not show a VM until Citrix DaaS initiates a power-on action for it. Then, the VM's status in Studio changes to **On**. There are two types of machines with the following differences:

- For a pooled machine, the operating system disk and write-back cache exist only when the VM exists. When you shut down a pooled machine in the console, the VM is not visible in the Azure portal. There’s a significant storage cost saving if you routinely shut down machines (for example, outside of working hours).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For a dedicated machine, the operating system disk is created the first time the VM is powered on. The VM in the Azure portal remains in storage until the machine identity is deleted. When you shut down a dedicated machine in the console, the VM is still visible in the Azure portal.

NOTE:

Support for Azure catalogs created before the on-demand provisioning feature (“legacy” catalogs) is deprecated. Therefore, recreate the Azure legacy catalog VMs. The catalogs are then provisioned as on-demand that saves storage cost.

Preserving a provisioned virtual machine when power cycling

Choose whether to preserve a provisioned virtual machine when power cycling. Use the PowerShell parameter `New-ProvScheme CustomProperties`. This parameter supports an extra property, `PersistVm`, used to determine if a provisioned virtual machine persists when power cycled. Set the `PersistVm` property to **true** to persist a virtual machine when powered off, or set the property to **false** to ensure that the virtual machine is not preserved when powered off.

NOTE:

The `PersistVm` property only applies to a provisioning scheme with the properties `CleanOnBoot` and `UseWriteBackCache` enabled. If the `PersistVm` property is not specified for non-persistent virtual machines, they’re deleted from the Azure environment when powered off.

In the following example, the `New-ProvScheme CustomProperties` parameter sets the `PersistVm` property to **true**:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

In the following example, the `New-ProvScheme CustomProperties` parameter preserves the write-back cache by setting `PersistVM` to **true**:

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

TIP:

The `PersistVm` property determines whether to preserve a provisioned virtual machine. The `PersistOsdisk` property determines whether to persist the OS disk. To preserve a provisioned virtual machine, preserve the OS disk first. You cannot delete the OS disk without first deleting the virtual machine. You can use the `PersistOsdisk` property without using specifying the `PersistVm` parameter.

Customize power on behavior at storage type change failure

At power on, the storage type of a managed disk can fail to change to the desired type due to a failure on Azure. In these scenarios, the VM would remain off with a failure message sent to you. However, you can either choose to power on the VM even when storage cannot be restored to its configured type or choose to keep the VM powered off.

- If you configure the custom property `FailSafeStorageType` as **true** (default setting) or do not specify it in `New-ProvScheme` or `Set-ProvScheme` commands:
  - On power on, the VM powers on with the incorrect storage type.
  - On shutdown, the VM remains off with the incorrect storage type.
- If you configure the custom property `FailSafeStorageType` as **false** in `New-ProvScheme` or `Set-ProvScheme` commands:
  - On power on, the VM remains off with the incorrect storage type.
  - On shutdown, the VM remains off with the incorrect storage type.

To create a machine catalog to include `FailSafeStorageType` custom property:

1. Open a PowerShell window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Create an identity pool if not already created.
4. Add the custom property in `New-ProvScheme`. For example:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. Create the machine catalog.

To update an existing machine catalog so to include `FailSafeStorageType` custom property. This update does not affect existing VMs.

1. Update the custom property in `Set-ProvScheme` command. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />

</CustomProperties>"
```

To apply the change done in Set-ProvScheme to the existing VMs, run the `Request-ProvVMUpdate` command.

1. Run the Request-ProvVMUpdate command. For example:

   ```
   Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <List-Of-
   Vm-Names>
   ```

2. Restart the VMs.

Create hibernation-capable VMs

In Azure environments, you can create an MCS machine catalog that supports hibernation. Using this feature, you can suspend a VM, and then reconnect to the previous state of the VM when a user signs in again.

The hibernation capability applies to the following:

- Single-session OS
- Persistent and non-persistent VMs
- Static and random (pooled) VDI desktops

You can resume to the same session after you hibernate a VM, irrespective of whether the VDI desktop is static or random.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this section, see the following:

- Prerequisites
- Limitations
- Create and manage a hibernation-capable machine catalog
- Create a machine catalog for existing hibernation-capable VMs
- Check the hibernation property
- Power management of VMs (Manual and Automated)

Prerequisites to use hibernation

To use hibernation, make sure to complete the following tasks:

- Install the Azure VM Agent on the master image for both Windows and Linux. The page file of the Windows image can be on the temporary disk. MCS sets the page file location to the C: drive in the base disk when hibernation is enabled on the machine catalog.
- MCS automatically sets the hibernation property for the generated resources. You do not need to configure properties of the master resources to support hibernation.
- Use a VM size in your subscription that supports hibernation.
- Create a hibernation-capable machine profile (VM or template spec) so that VMs inherit the hibernation-capability. To create the VM, see Getting started with hibernation.

  NOTE:

  As per Microsoft, you can deploy hibernation enabled VMs from an OS disk. This feature is supported for certain regions currently and will be available for all the regions soon. For more information, see Deploy hibernation enabled VMs from an OS disk.

  To create the template spec, do the following:

  a. Open the Azure Portal. Choose a VM whose configuration you want to use in the template. Select **Export template** in the left pane.

  b. Clear the **Include parameters** checkbox. Copy the context and save it as a JSON file, for example, `VMExportTemplate.json`.

  c. Ensure that the parameter `hibernationEnabled` is `true` on the template. If the parameter is not `true`, check the VM configuration that you used. You can specify a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

supported VM size in the template file. However, you can also specify the machine size while creating the catalog.

d. Add the template for the network interface resource to the JSON file `VMExportTemplate.json`. As a result, you have an ARM template file having two resources.

e. Select **Azure Portal > Template specs > Import template > Choose local template file** to import this template file as an ARM template spec.

f. After the ARM Template specification is created, you can use it as a machine profile.

> **NOTE:**
>
> It might take a few minutes to sync to Citrix Studio.

For more information, see the Microsoft document Prerequisites to use hibernation.

Limitations

- Only single-session OS machine catalogs (persistent and non-persistent) are supported.
- Ephemeral OS disks and MCS I/O features do not support Azure hibernation.
- Hibernation might fail during the Automatic Windows updates.
- Trusted Launch is a prerequisite for hibernation when Hyper-V is enabled.

For more information, see the Microsoft document.

Create and manage a hibernation-capable machine catalog

To create hibernation-capable VMs, you can create and manage a hibernation-capable machine catalog using:

- Studio
- PowerShell commands

CREATE A CATALOG USING STUDIO

1. Sign in to Citrix Cloud.
2. In the **DaaS** tile, click **Manage** to open Studio.
3. In the left pane, select **Machine Catalogs**.
4. Select **Create Machine Catalog**. The catalog creation wizard opens.
5. On the **Machine Type** page, select the **Single-session OS** machine type for this catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. On the **Machine Management** page, select the settings as follows:
    a. Select **Machines that are power managed (for example, virtual machines or blade PCs)**.
    b. Select **Citrix Machine Creation Services™ (MCS)**.
    c. Select a resource location from the **Resources** drop-down list.
7. On the **Desktop Experience** page, select the random or static desktop experience as needed.
8. On the **Image** page, select a master image. Select the checkbox **Use a machine profile** and select a machine profile that supports hibernation. Click the tooltip to know if a machine profile supports hibernation.

    NOTE:

    If you select an Azure-managed master image, only images in the same region as the selected resource location are displayed.

9. On the **Storage and License Types** page, select the storage and license to use for this catalog.
10. On the **Virtual Machines** page, select the count of VMs, VM size, and availability zone.

    NOTE:

    The machine sizes that support hibernation are only shown for your selection.

11. On the **NICs** page, add the NICs you want the VMs to use.
12. On the **Disk Settings** page, select the storage type and size of the write-back cache disk.
13. On the **Resource Group** page, select the resource group to provision VMs.
14. On the **Machine Identities** page, select **Create new Active Directory accounts**. Then, specify an account naming scheme.
15. On the **Domain Credentials** page, click **Enter credentials**. Enter your domain credentials to perform account creation in the target Active Directory domain.
16. On the **Summary** page, enter a name for the machine catalog, and then click **Finish**.

When the MCS machine catalog creation is complete, locate the catalog in the catalog list, and then click the **Template Properties** tab. The value of the parameter **Hibernation** must be **Supported**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you want to edit a machine catalog, consider the following restrictions:

- If the current machine catalog supports hibernation, you can't:
  - Change the VM size to a hibernate-incapable one.
  - Change the machine profile to a hibernate-incapable one.
- If the current machine catalog does not support hibernation, you can't:
  - currently, change the machine profile to a hibernate-capable one using Studio.

CREATE A MACHINE CATALOG FOR MANAGING EXISTING HIBERNATION-CAPABLE VMS

If you already have hibernation-capable VMs and want to suspend and resume them, create a machine catalog to import those VMs for power management.

> **NOTE:**
>
> You can create a machine catalog containing both hibernation-capable and incapable VMs. However, if you want hibernation-related functionality, you must create the machine catalog with only hibernation-capable VMs.

To create a catalog for existing hibernation-capable VMs using Studio, follow the on-screen instructions to complete the steps and pay attention to the following key settings:

1. On the **Machine Management** page, select **Machines that are power managed**, and then select **Other service or technology** as the way of deploying machines.
2. On the **Virtual Machines** page, add or import only the hibernation-capable VMs.

CREATE A MACHINE CATALOG USING POWERSHELL COMMANDS

After you meet all the requirements to use hibernation, you can create a hibernation-capable machine catalog using the `New-ProvScheme` command. For information on how to create a catalog using the Remote PowerShell SDK, see Manage Citrix DaaS using Remote PowerShell SDKs.

While creating the catalog, you can check whether a VM size and machine profile supports hibernation or not using the following PowerShell commands:

- For the VM size, run the following command and check whether the property `supportsHibernation` is **True**. For example,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <VirtualNetwork>
\serviceoffering.folder") | select Name, AdditionalData | ConvertTo-
Json
```

- For the machine profile, run the following command and check whether the property `supportsHibernation` is **True**. For example,

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

If you want to edit a machine catalog, consider the following restrictions:

- If the current machine catalog supports hibernation, you can't:
  - Change the VM size to a hibernate-incapable one
  - Change the machine profile to a hibernate-incapable one
- If the current machine catalog does not support hibernation, you can't:
  - currently, change the machine profile to a hibernate-capable one using Studio.

For information on how to modify VM size and machine profile of a catalog using the Remote PowerShell SDK, see `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`.

Check hibernation property

You can check the hibernation property of a machine catalog, VM, and a broker machine using the PowerShell commands:

- To check the hibernation property of a provisioning scheme, run the following PowerShell commands. The `HibernationEnabled` parameter must be `True`.

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- To check the hibernation property of a provisioning VM, run the following PowerShell commands. The `SupportsHibernation` parameter must be `True`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- To check the hibernation capacity of a broker machine, run the following PowerShell commands. The **Suspend** and **Resume** power actions indicate hibernation capability.

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

Power management of hibernation-capable VMs

You can perform the following power management operations on the hibernation-capable VMs:

- **Suspend** VM from the running state
- **Resume** VM from the suspended state
- **Force shut** down VM from a suspended state
- **Force restart** the VM from the suspended state

See the following for more information:

- Suspend
- Resume

SUSPEND

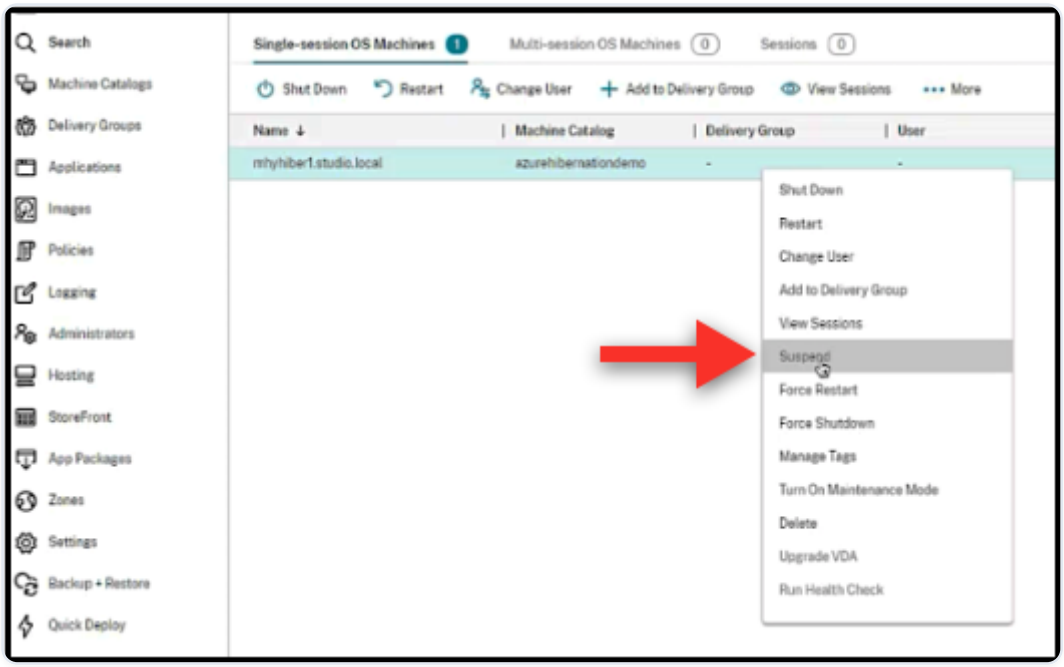
You can suspend a VM using one of the following ways:

- **Manually** using Studio
- **Automatically** using the timeout policy: For more information, see Miscellaneous settings.

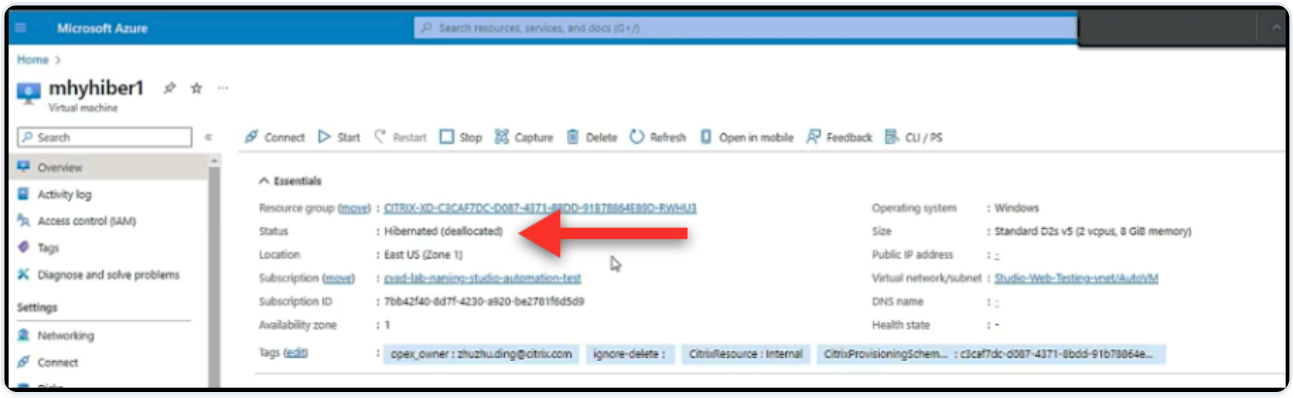
To manually suspend a VM:

1. Right-click the VM, and select **Suspend**. Click **Yes** to confirm the action. The **Power State** changes from **Suspending** to **Suspended**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can check the status of the VM in the Azure portal.

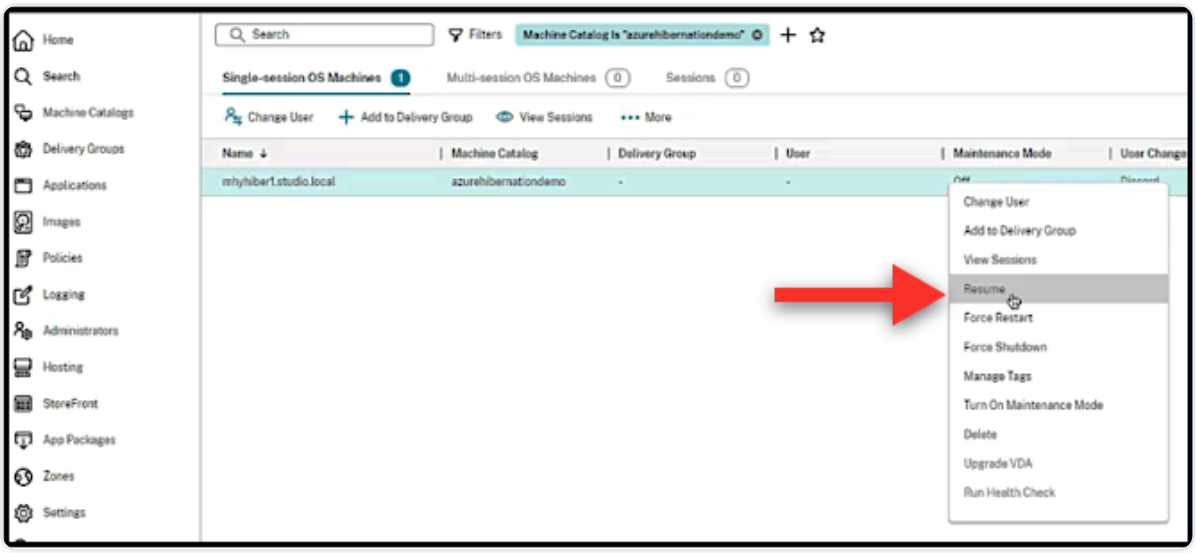


RESUME

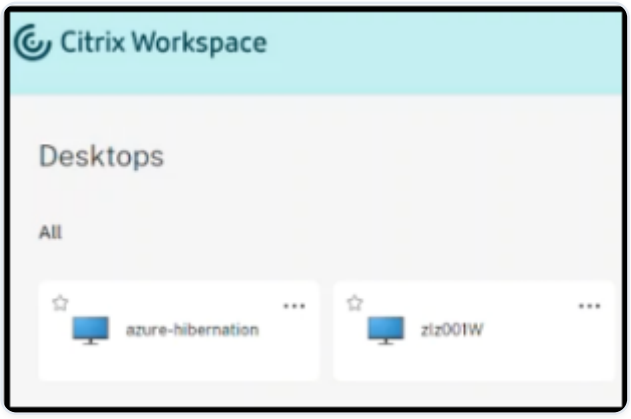
To resume a hibernated VM, use one of the following ways:

- **Manually**:
  - Administrators can resume the VM using Studio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

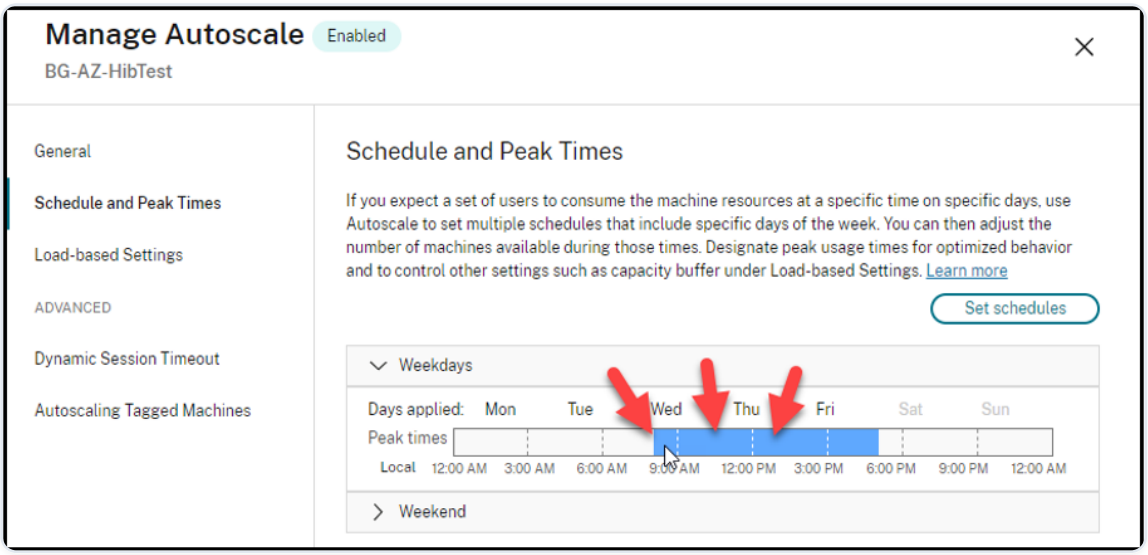


- When end users launch the desktop, it automatically resumes.

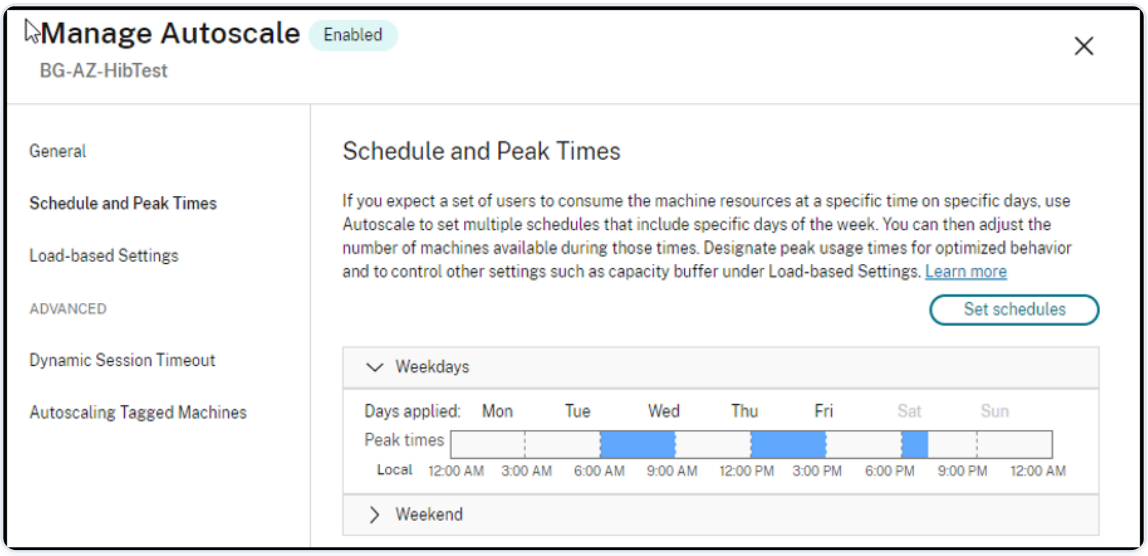


- **Automatically**:
  - Autoscale™ can automatically power on the hibernated machines if you configure the peak times correctly. You can set the peak times in 30-minutes intervals by clicking the time-schedule. Each blue frame represents a timeslot marked as peak time. The peak times can have consecutive and non-consecutive time slots.
    - Consecutive time slots

© 1997–2026 Citrix Systems, Inc. All rights reserved.



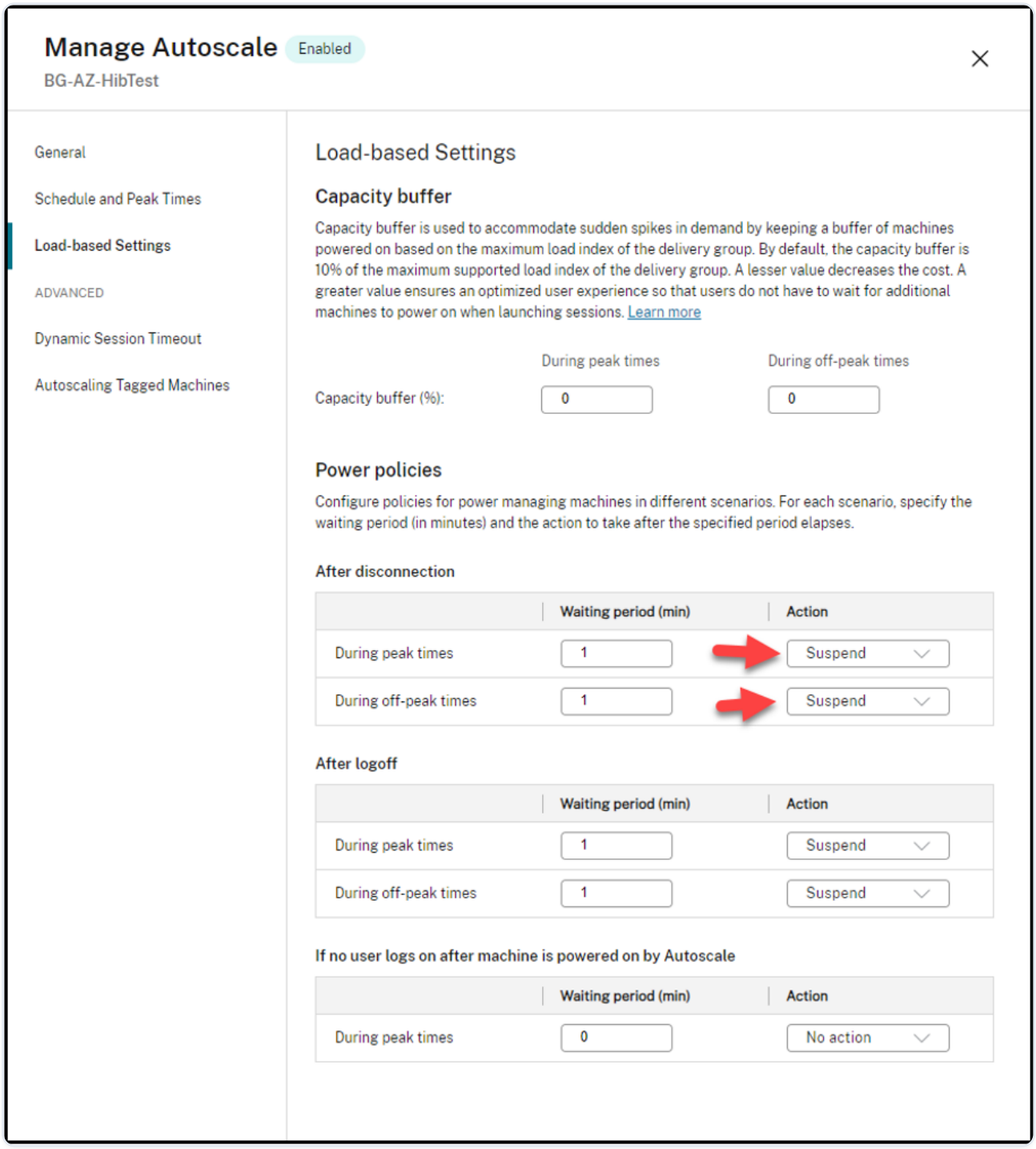
- Non-consecutive time slots



NOTE:

In **Manage Autoscale > Load-based Settings**, if the **Action** is configured as **Suspend**, then make sure that all VMs within that delivery group have hibernation capability. Otherwise, VMs that can’t hibernate continues to run.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Get warnings messages for hibernation failure

You can get warning messages using a PowerShell command `Get-ProvOperationEvent` in case of hibernation failure of MCS-provisioned and existing hibernation-capable VMs. For information about the Powershell command, see the SDK documentation Get-ProvOperationEvent.

To do this:

1. Open a PowerShell window.
2. Run `asnp citrix*` to load Citrix-specific PowerShell modules.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Run `Get-ProvOperationEvent` to get the warning message in case of hibernation failure.

```
Get-ProvOperationEvent -filter { OperationName -eq "Suspend" }
```

Output:

```
EventAdditionalData : Error code = OperationNotAllowed and Error
message = The Hibernate-Deallocate Operation cannot be performed on a
VM that has extension 'AzureHibernateExtension' in failed state. For
more information, see https://aka.ms/hibernate-resume/errors. Error
details from the extension : Enabling

                  hibernate failed. Response from the powercfg command.
Exit Code: 1. Error message:

                  Hibernation failed with the following error: The
request is not supported.



                  The following items are preventing hibernation on
this system.

                    The current Device Guard configuration has disabled
hibernation.

                    An internal system component has disabled
hibernation.

                            Hypervisor

                  Status: 409

                  ErrorCode: OperationNotAllowed



                  Content:

                  {

                    "error": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    "code": "OperationNotAllowed",

                    "message": "The Hibernate-Deallocate Operation
cannot be performed on a VM that has extension
'AzureHibernateExtension' in failed state. For more information, see
https://aka.ms/hibernate-resume/errors. Error details from the
extension : Enabling hibernate failed. Response from the

                powercfg command. Exit Code: 1. Error message:
\nHibernation failed with the following error: The request is not
supported.\r\r\n\r\nThe following items are preventing hibernation on
this system.\r\n\tThe current Device Guard configuration has disabled
hibernation.\r\n\tAn internal system

                component has disabled hibernation.
\r\n\t\tHypervisor"

                  }

                }

EventCategory       : Warning

EventDateTime       : 1/11/2024 4:18:31 AM

EventId             : 0

EventMessage        : Failed to suspend machine my-resource-group/my-
vm.

EventSeverity       : Important

EventSource         : AzureRmPlugin

EventState          : New

LinkedObjectType    : ProvisioningScheme

LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366

OperationName       : Suspend

OperationTargetName : my-resource-group/my-vm
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
OperationTargetType : VirtualMachine

OperationType       : PowerManagement

Recommendation      :
```

TROUBLESHOOTING HIBERNATION ISSUES

You get the following error message if you try to enable both hibernation and trusted launch VM features, however, configuration of the guest OS is not correct.

ERROR CODE	ERROR MESSAGE
OperationNotAllowed	The Hibernate-Deallocate Operation cannot be performed on a VM that has extension 'AzureHibernateExtension' in failed state. For more information, see `<https://aka.ms/hibernate-resume/errors/>`. Error details from the extension : Enabling hibernate failed. Response from the powercfg command. Exit Code: 1. Error message: Hibernation failed with the following error: The request is not supported. The following items are preventing hibernation on this system. **The current Device Guard configuration has disabled hibernation. An internal system component has disabled hibernation**.

To resolve the issue, ensure that virtualization is enabled within the guest VM. For example, confirm that Hyper-V is enabled in a Windows environment.

For more information on warning messages, see the Microsoft document Troubleshooting VM hibernation.

NOTE:

Error messages related to failure in resuming a VM will be available in a future release.

More information

For more information on Citrix Azure hibernation, see the Citrix Tech Zone article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Power manage Nutanix AHV VMs

With Citrix DaaS™, you can power manage Nutanix AHV VMs. Use the **Search** node in the navigation pane to find the machine you want to power manage.

You can use the following power actions:

- Start
- Shut Down
- Force Shutdown
- Force Restart
- Restart

NOTE:

- Reset, Suspend, and Resume power actions are not supported.
- Shut Down or Restart: The VM might not respond to the shutdown request if active users or running programs interrupt the shutdown, or if the OS requires updates. To ensure that guest shutdown and restart work properly on Windows VMs, apply the recommended power action settings on the VDA, such as screen saver and display power settings. For more information, see Nutanix KB.

Security policies

This article describes security features on various supported hypervisors. The security features include:

- Security group
- Secure boot
- Encryption capabilities

Security group

Security group is a group of security rules to filter network traffic between resources in a virtual network. The security rules allow or deny inbound network traffic to, or outbound network traffic from, several types of resources. Each rule specifies the following properties:

- Name: A unique name within the network security group

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Priority: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority
- Source or Destination: Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or application security group
- Protocol: The protocols based on which you add rules for each security group
- Direction: Whether the rule applies to inbound, or outbound traffic
- Port range: You can specify an individual or range of ports
- Action: Allow or deny

See the following for more information on supported hypervisors:

- Security group in AWS
- Security group in Microsoft Azure
- Security group in Google Cloud Platform

Security group in AWS

Security groups act as virtual firewalls that control traffic for the instances in your VPC. You add rules to your security groups that allow instances in your public subnet to communicate with instances in your private subnet. You can also associate these security groups with each instance in your VPC. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance.

For more information on the network setting during image preparation, see Network setting during image preparation.

When you launch an instance, you can specify one or more security groups. To configure security groups, see Configure security groups.

Security group in Microsoft Azure

Citrix DaaS supports network security groups in Azure. Network security groups are expected to associate with subnets. For more information, see Network security groups.

For more information on network security group created during image preparation, see Create a machine catalog using an Azure Resource Manager image.

Security group in Google Cloud Platform

During the preparation of a machine catalog, a machine image is prepared to serve as the master image system disk for the catalog. When this process occurs, the disk is temporarily attached to a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

virtual machine. This VM must run in an isolated environment that prevents all inbound and outbound network traffic. This is accomplished through a pair of deny-all firewall rules. For more information, see Firewall Rules.

Secure Boot and vTPM

Secure Boot is a feature of the Unified Extensible Firmware Interface (UEFI), which is responsible for booting the system. It ensures that only trusted software is loaded during the boot process.

Trusted Platform Module (TPM) is a hardware chip that provides secure storage for cryptographic keys and other sensitive data. A Virtual Trusted Platform Module (vTPM) performs the same functions as a TPM, but it performs cryptographic coprocessor capabilities in software. While TPM can enhance security, it's not a requirement for Secure Boot.

See the following for more information on supported hypervisors:

- Secure Boot and NitroTPM in AWS
- Secure Boot and vTPM in Google Cloud Platform
- Secure Boot and vTPM in Microsoft Azure
- Secure Boot and vTPM in Nutanix Prism Central
- vTPM in VMware
- Secure Boot and vTPM for XenServer
- Secure Boot and vTPM in SCVMM

Secure Boot and NitroTPM in AWS

In AWS environments, you can select a master image (AMI) with NitroTPM and/or UEFI secure boot enabled. Accordingly, the provisioned VMs in the catalog are also enabled with NitroTPM and/or UEFI secure boot. This implementation ensures that the VMs are secured and trusted. For more information on NitroTPM and UEFI Secure Boot, see the Amazon documentation. For creating a catalog enabled with NitroTPM and UEFI secure boot, see Enable NitroTPM and UEFI secure boot for VM instances.

Secure Boot and vTPM in Google Cloud Platform

You can provision shielded virtual machines on Google Cloud Platform (GCP). Shielded VM's verifiable integrity is achieved by using the following features:

- Secure Boot
- vTPM-enabled Measured Boot

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Integrity monitoring

For more information on using PowerShell to create a catalog with shielded VM, see Using PowerShell to create a catalog with shielded VM.

NOTE:

If you install Windows 11 on the master image, then you must enable vTPM during the master image creation process. Also, if you use a machine profile for creating the catalog, then you must enable vTPM on the machine profile source (VM or instance template). For information on creating Windows 11 VMs on the sole-tenant node, see Create Windows 11 VMs on the sole-tenant node.

Secure Boot and vTPM in Microsoft Azure

In Azure environments, you can create machine catalogs enabled with Trusted Launch. Azure offers Trusted Launch as a seamless way to improve the security of generation 2 VMs. Trusted Launch protects against advanced and persistent attack techniques. To enable Trusted Launch, use a machine profile-based catalog configuration. At the root of Trusted Launch is Secure Boot for your VM. Trusted Launch also uses the vTPM to perform remote attestation by the cloud. This is used for platform health checks and for making trust-based decisions. You can individually enable Secure Boot and vTPM. For more information on creating a machine catalog with Trusted Launch, see Machine catalogs with Trusted Launch.

Secure Boot and vTPM in Nutanix Prism Central

MCS supports creating a machine catalog with vTPM, UEFI, and secure boot with Nutanix Prism Central. You can select a master image (template) with vTPM and UEFI secure boot enabled.

In Nutanix Prism Central, UEFI Secure Boot does not require vTPM. However, to link a vTPM to a VM, the VM must be UEFI booted, irrespective of whether Secure Boot is enabled or not.

Furthermore, vTPM, UEFI, and secure boot enabled VMs can be imported from Nutanix Prism Central and can be power managed by Citrix DaaS.

Nutanix provides support for vTPM and UEFI Secure Boot. See:

- vTPM (Virtual Trusted Platform Module) support on AHV.
- Secure Boot Support for VMs
- Securing AHV VMs with a Virtual Trusted Platform Module

© 1997–2026 Citrix Systems, Inc. All rights reserved.

vTPM in VMware

MCS supports creating a machine catalog with vTPM. If windows 11 is installed on the master image, then it is a requirement to have vTPM enabled for the master image. If machine profile-based configuration is used and vTPM is enabled, then VMs in the catalog inherit the same vTPM content from the VM template. If the machine profile is not used and the master image is vTPM enabled, then VMs in the catalog have blank vTPM. For more information, see Create a machine catalog using a machine profile.

Secure Boot and vTPM for XenServer®

XenServer provides UEFI Secure Boot on some of its supported VM operating systems. Secure Boot prevents unsigned, incorrectly signed or modified binaries from being run during boot. On a UEFI-enabled VM that enforces Secure Boot, all drivers must be signed. For more information, see Guest UEFI and Secure Boot.

In XenServer 8, vTPM is not required for UEFI Secure Boot. However, to link a vTPM to a VM, that VM must be UEFI booted, whether Secure Boot is enabled or not. Windows 11 VM requires a linked vTPM and it is created automatically when the Windows 11 VM is created from the provided template. For other operating systems, a vTPM is optional. For more information, see vTPM.

MCS supports creating a machine catalog with vTPM. If machine profile-based configuration is used and vTPM is enabled, then VMs in the catalog inherit the same vTPM content from the VM template. If the machine profile is not used and the master image is vTPM enabled, then VMs in the catalog will inherit the same vTPM content as the master image.

Secure Boot and vTPM in SCVMM

In System Center Virtual Machine Manager (SCVMM) environments, you can select a master image and machine profile with vTPM and/or Secure Boot enabled. As a result, the catalog provisions VMs with vTPM and/or Secure Boot enabled. This implementation secures the VMs and keeps them trusted. To create a catalog with vTPM and Secure Boot enabled, see create a catalog with a machine profile.

Encryption capabilities

Encryption capabilities protect the content of virtual machines from attacks by malicious guests on a shared virtual machine host and from attacks launched by the hypervisor control software that manages all the virtual machines on the host.

See the following for more information on supported hypervisors:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Encryption capabilities in AWS
- Encryption capabilities in Google Cloud Platform
- Encryption capabilities in Microsoft Azure

Encryption capabilities in AWS

This section describes the encryption capabilities in AWS virtualization environments.

Automatic encryption

You can turn on automatic encryption of new Amazon EBS volumes and snapshot copies created in your account. For more information, see Automatic encryption.

Encryption capabilities in Google Cloud Platform

This section describes the encryption capabilities in Google Cloud Platform (GCP) virtualization environments.

If you need more control over key operations than what Google-managed encryption keys allows, you can use customer-managed encryption keys. When using a customer-managed encryption key, an object is encrypted with the key by Cloud Storage at the time it's stored in a bucket, and the object is automatically decrypted by Cloud Storage when the object is served to requesters. For more information, see Customer-managed encryption keys.

You can use Customer Managed Encryption Keys (CMEK) for MCS catalogs. For more information, see Using Customer Managed Encryption Keys (CMEK).

Encryption capabilities in Microsoft Azure

This section describes the encryption capabilities in Azure virtualization environments.

Azure server side encryption

Most Azure managed disks are encrypted with Azure Storage encryption, which uses server-side encryption (SSE) to protect your data and to help you meet your security and compliance commitments. Citrix DaaS supports customer-managed encryption keys for Azure managed disks through Azure Key Vault. For more information, see Azure server side encryption.

Azure disk encryption at host

You can create an MCS machine catalog with encryption at host capability.

This encryption method does not encrypt the data through the Azure storage. The server hosting the VM encrypts the data and then the encrypted data flows through the Azure storage server. Hence, this method of encryption encrypts data end to end.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on creating MCS machine catalog with encryption at host capability, see Azure disk encryption at host.

Azure double encryption

Double encryption is platform-side encryption (default) and customer managed encryption (CMEK). Therefore, if you are a high security sensitive customer who is concerned about the risk associated with any encryption algorithm, implementation, or a compromised key, you can opt for this double encryption. Persistent OS and data disks, snapshots, and images are all encrypted at rest with double encryption. For more information, see Double encryption on managed disk.

Azure confidential VMs

Azure confidential computing VMs ensure that your virtual desktop is encrypted in memory and protected in use.

You can use MCS to create a catalog with Azure confidential VMs. You must use the machine profile workflow to create such a catalog. You can use both VM and ARM template spec as a machine profile input.

For more information, see Azure confidential VMs.

Service Window

The Service Window feature provides a capability to schedule and automate operations on MCS-provisioned VMs. This feature currently supports various operations such as Reset OS disk and hardware configuration changes. You can schedule these operations and return later to verify completion, rather than performing updates manually.

You can schedule operations for either a specific list of VMs or an entire machine catalog. Each operation runs at the time specified. Multiple operations can be scheduled for the same VM. However, you cannot schedule more than one hardware update for a single VM.

You can also:

- Add a description for the Service Window.
- Provide a detailed message to be displayed to any users who are logged on when the operation runs.
- Configure how many buffer minutes are granted to save work for the logged on users before the operation is forcibly executed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Advantages

Improved user experience and continuity

- **Graceful session handling**: Instead of abrupt disconnections, you can define a professional notification to save the work before the VM is powered down.
- **Scheduled downtime**: You can move heavy update tasks to off-peak hours (for example, 2:00 AM) without requiring you to manually log in at that time.
- **Cost-efficient hardware updates**: Updating hardware using Service Window saves significant costs on large implementations. This feature automatically analyses if a VM requires a reboot to apply settings. Therefore, by avoiding unnecessary reboots, Service Window minimize these expenses.

Advanced hardware flexibility

- **Update hardware configurations**: Use Service Window to schedule the hardware updates. The system intelligently manages the update flow, checking for reboot necessity and handling session log-offs, ensuring that your catalog evolves to meet new resource demands with zero manual oversight.
- **Flexible SKU reconfiguration**: Easily update SKUs, which previously required manual recreation of the catalog.
- **Hibernation support for existing VMs**: Overcomes the "temporary disk" limitation. The Service Window allows the MCSIO driver to relocate the pagefile to the C: Drive and enable hibernation properties on VMs that were already deployed.

Important consideration

- **User notification**: Logged on users receive an initial alert regarding the Service Window operation, ensuring they have sufficient time to save their work. Once the notification period expires, the machine automatically powers down to perform the operation.

Limitataion

The WBC disk size can't be changed on the existing VMs. It could be applied to the machine catalog for the new VMs.

Service Window operations

The Service Window currently supports OS disk resets and hardware configuration changes using PowerShell.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PowerShell commands: Generic commands are outlined in this article, while detailed, hypervisor-specific scripts can be found on our GitHub page `<https://github.com/citrix/citrix-mcs-sdk-samples/>`.

Reset OS disk

OS disk resets can be done using the PowerShell command `New-ProvMaintenanceCycle`. The commands creates a new Service Window for an entire catalog or specific VMs. The cycle starts at the time you specify in `ScheduledStartTimeInUTC`. You also provide `MaxDurationInMinutes`, which indicates the maximum time the Service Window can run.

Example: Reset OS disk for specific VMs

```
New-ProvMaintenanceCycle -Operation ResetOSDisk
-MaintenanceCycleDescription "Resetting Boot Disk" -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -PurgeDBAfterInDays
1 -SessionWarningTimeInMinutes 15 -SessionWarningLogOffTitle "Scheduled
Maintenance" -SessionWarningLogOffMessage "There is a scheduled
maintenance coming up and involves turning off the machine, please save
your work and log out, Thank You" -VMName VDA02,VDA03
```

Example: Reset OS disk for the entire catalog

```
New-ProvMaintenanceCycle -Operation ResetOSDisk
-MaintenanceCycleDescription "Resetting Boot Disk" -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -PurgeDBAfterInDays
1 -SessionWarningTimeInMinutes 15 -SessionWarningLogOffTitle "Scheduled
Maintenance" -SessionWarningLogOffMessage "There is a scheduled
maintenance coming up and involves turning off the machine, please save
your work and log out, Thank You" -AllVMs
```

Update hardware settings

Schedule hardware updates using Service Window, thereby having full control over when the changes take effect. You can choose to target only the newly created VMs, an entire catalog (new and existing VMs), or specific VMs as needed.

- To update hardware settings for new VMs or entire catalog, select a provisioning scheme version and run the PowerShell command `New-ProvSchemeHardwareUpdate`. You can apply a previously created provisioning scheme version to VMs. You can also enable hibernation on a VM with temporary disk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To update hardware settings for specific VMs, select a VM configuration version, and run the PowerShell command `New-ProvVmHardwareUpdate`.

Important considerations

- New machines added to a catalog after scheduling a hardware update continues to be created with older specifications until the specified UTC time for applying new specifications.
- A single validation failure during the Service Window creation prevents the cycle from being created and return an error message.
- For enabling hibernation, consider the following:
  - The VDA version must be greater than 2503.
  - Machine Creation Services I/O (MCSIO) must be installed.
  - The machine profile must support hibernation.
  - The VM SKU and operating system must support hibernation.
  - If VBS is enabled, Hyper-V must also be enabled. Nested virtualization requires Trusted Launch on the VM.
  - The free OS disk size must be larger than the VM's memory size.

Schedule hardware updates on an entire machine catalog or new VMs

1. Run `New-ProvSchemeVersion` to create a new provisioning scheme version with updated hardware settings. For more information, see the SDK doc.
2. Run the PowerShell command `New-ProvSchemeHardwareUpdate` to schedule a Service Window for hardware updates as specified in the provisioning scheme version.

Example: `AllVMs` (new and existing) in the machine catalog are considered for the update:

```
New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 4
-MaintenanceCycleDescription "Updating RAM and CPU Count to 8GB and 4"
-StartsNow -MaxDurationInMinutes 100 -ProvisioningSchemeName CVC
-PurgeDBAfterInDays 1 -SessionWarningTimeInMinutes 15
-SessionWarningLogOffTitle "Scheduled Maintenance"
-SessionWarningLogOffMessage "There is a scheduled maintenance coming up
and involves turning off the machine, please save your work and log out,
Thank You" -AllVMs
```

Example: `NewVMsOnly` (new and existing) in the machine catalog are considered for the update:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 4
-MaintenanceCycleDescription "Updating RAM and CPU Count to 8GB and 4"
-StartsNow -MaxDurationInMinutes 100 -ProvisioningSchemeName CVC
-PurgeDBAfterInDays 1 -SessionWarningTimeInMinutes 15
-SessionWarningLogOffTitle "Scheduled Maintenance"
-SessionWarningLogOffMessage "There is a scheduled maintenance coming up
and involves turning off the machine, please save your work and log out,
Thank You" -NewVMsOnly
```

Run `Get-ProvSchemeHardwareUpdate` to retrieve Service Window objects associated with hardware scheme updates. Example:

```
Get-ProvSchemeHardwareUpdate -MaintenanceCycleId xxxx-xxxx-yyyy-zzzz
```

Schedule hardware updates on specific VMs

1. Run `New-ProvVmConfiguration` to create a new provisioning VM configuration. For more information, see the SDK doc.
2. Run the PowerShell command `New-ProvVmHardwareUpdate` to schedule a Service Window for hardware updates as specified in the VM configuration version.

NOTE:

For each VM, any personalized settings (VM configuration version) always take precedence over the specifications defined in the provisioning scheme version. If a particular setting is not personalized on the VM, its value is inherited from the associated provisioning scheme version.

Example:

```
New-ProvVmHardwareUpdate -ProvVmConfigurationVersion 4 -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -VMName AbcTest01
```

Run `Get-ProvVmHardwareUpdate` to retrieve Service Window objects associated with hardware VM updates. Example:

```
Get-ProvVmHardwareUpdate -MaintenanceCycleId xxxx-xxxx-yyyy-zzzz
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also remove a personalization used to create provisioning VM versions using `Remove-ProvVmConfiguration` command. Example:

```
Remove-ProvVmConfiguration -Version 2 -VMName AbcTest01
```

Miscellaneous PowerShell commands associated with Service Window

- `Get-ProvMaintenanceCycle`: Retrieves information of all the Service Windows. Example:

  ```
  Get-ProvMaintenanceCycle -MaintenanceCycleId
  10073b8e-7e94-4527-8580-0e448eae0ad1
  ```

- `Get-ProvMaintenanceCycleVM`: Retrieves information of each Service Window operation for individual VMs, along with its status. Example:

  ```
  Get-ProvMaintenanceCycleVM -MaintenanceOperation HardwareUpdate
  -VirtualMachineSid 42263076-44ae-1ff9-f58b-62d57ddf8db5
  ```

  The various Service Window statuses are:

  - Running
  - Failed
  - Completed
  - Cancelling
  - Cancelled
  - NotProcessed
  - Pending
  - Incomplete
  - Repaired
  - Recovering

- `Remove-ProvMaintenanceCycle`: Removes a Service Window when the Service Window is not active. Example:

  ```
  Remove-ProvMaintenanceCycle -MaintenanceCycleId
  867af1ba-5b72-402e-9dc3-033298248f8e
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Cancel-ProvMaintenanceCycle`: If the operation has not yet started by MCS on a VM, then this PowerShell command cancels the operation. MCS does not cancel an operation that is currently running on the VM. Example:

  ```
  Cancel-ProvMaintenanceCycle -MaintenanceCycleId
  867af1ba-5b72-402e-9dc3-033298248f8e
  ```

- `Restart-ProvMaintenanceCycle`: If a Service Window has failed or is incomplete due to external causes, such as the hypervisor being down or insufficient time, this command helps restart the cycle and process any failed or not-processed jobs. Example:

  ```
  Restart-ProvMaintenanceCycle -MaintenanceCycleId
  4f363b78-458a-403a-82e5-7fcc6caa498b -ScheduledStartTimeInUTC "June
  19th 2024, 6AM" -MaxAllocatedDurationInMinutes 400
  ```

- `Update-ProvMaintenanceCycle`: If a Service Window is already scheduled and has not started, this command alters certain parameters.

  Example: Update maximum duration:

  ```
  Update-ProvMaintenanceCycle -MaintenanceCycleId
  4f363b78-458a-403a-82e5-7fcc6caa498b -MaxDurationInMinutes 100
  ```

  Example: Update VMs for a provisioning scheme:

  ```
  Update-ProvMaintenanceCycle -MaintenanceCycleId
  4f363b78-458a-403a-82e5-7fcc6caa498b -ProvisioningSchemeUid
  867af1ba-5b72-402e-9dc3-033298248f8e -VMName ncn01,ncn02
  ```

Load balance machines

Load balancing helps organizations achieve the cost balance they want while being able to take advantage of all the cloud has to offer. Load balancing is configured at the delivery group level.

NOTE:

Load balancing applies only to multi-session OS machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Load balancing has two options:

- Horizontal load balancing
- Vertical load balancing

By default, horizontal load balancing is enabled.

Horizontal load balancing: In the horizontal load balancing model, the incoming user session is assigned to the least-loaded machine available. Consider this example, in a deployment, let's assume we have two VDAs. One has an active user session (User 1), and the second user (User 2) is waiting for a session. The horizontal load balancing algorithm assigns User 2 to VDA 2 because of the more favorable load index. Thus, the horizontal algorithm distributes sessions across all available VDAs, which might hinder machines from turning off when the load decreases.

Vertical load balancing: In the vertical load balancing model, the sessions are assigned to the VDAs with the highest load index. This helps consolidate the incoming user sessions to VDAs that are already being used by other users and helps to reduce the number of VDAs that must be powered on and kept ready for user sessions. Let's consider the same deployment as the one mentioned in the horizontal load balancing. User 1 is assigned to VDA 1, and the vertical load balancing algorithm is applied to the User 2 session. User 2 is assigned to VDA 1 because the higher load index is on VDA 1. Therefore, all incoming sessions are assigned to the most-loaded VDA until the high load index watermark is met. Only then, the other VDA starts receiving sessions.

Load balancing setting at site level

You can configure load balancing for all delivery groups (site-wide setting).

To configure this feature from Studio, select **Settings** in the left pane and the **Site settings** tab. Select an option under **Load Balancing Sessions on Machines**.

Alternatively, you can use PowerShell to enable or disable vertical load balancing site-wide. Use the `UseVerticalScalingForRdsLaunches` setting in the `Set-BrokerSite` cmdlet. Use `Get-BrokerSite` to display the value of the `UseVerticalScalingForRdsLaunches` setting. See the cmdlet help for details.

TIP:

To specify the maximum number of sessions a machine can host, use the Maximum number of sessions policy setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Load balancing setting at delivery group level

You can configure load balancing at the delivery group level and override the load balancing setting inherited from the site level.

You can configure this during creating a delivery group or editing an existing delivery group. See Step 2. Load balancing.

Load management

Load management measures the server load and determines which server to select under the current environment conditions. This selection is based on:

- **Server maintenance mode status**: A multi-session OS machine is considered for load balancing only when maintenance mode is off.
- **Server load index**: Determines how likely a server delivering multi-session OS machines is to receive connections. The index is a combination of load evaluators: the number of sessions and the settings for performance metrics such as CPU, disk, and memory use. Load evaluators are specified in load management policy settings. By default, the load index only uses the number of sessions in its calculation, and not CPU, disk, or memory until they are configured in load management policy settings. For information on policy settings, see Load management policy settings.

  A server load index of 10000 indicates that the server is fully loaded. If no other servers are available, users might receive a message that the desktop or application is currently unavailable when they launch a session. You can monitor the load index in Director (Monitor), a Studio search, and the SDK.

  In console displays, to display the **Server Load Index** column (which is hidden by default), select a machine, right-click a column header, and then select **Select Column**. In the **Machine category**, select **Load Index**.

  In the SDK, use the `Get-BrokerMachine` cmdlet. For details, see CTX202150.
- **Concurrent logon tolerance policy setting**: The maximum number of concurrent requests to log on to the server. (This setting is equivalent to load throttling in XenApp 6.x versions.)

  When all servers are at or higher than the concurrent logon tolerance setting, the next logon request is assigned to the server with the lowest pending logons. If more than one server meets these criteria, the server with the lowest load index is selected. See Concurrent logon tolerance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP:

To enforce the logon tolerance setting and cause concurrent logons that exceed the specified number to fail, you can run `Set-BrokerServiceConfigurationData Core.LogonToleranceIsHardLimit -SettingValue $true`.

Create delivery groups

Introduction

A delivery group is a collection of machines chosen from one or more machine catalogs. Delivery groups define which users can access those machines, and the applications and desktops available to them.

Creating a delivery group is the next step after setting up your site and machine catalogs. You can later modify the initial settings or create additional delivery groups as needed.

Some features and settings are only configurable when editing an existing delivery group. For more details, see Manage delivery groups.

Before you begin

Before creating a delivery group:

- Review this article to understand the required choices and information.
- Ensure that you have created a connection to the hypervisor, cloud service, or other resource hosting your machines.
- Make sure a machine catalog with virtual or physical machines is available.

Pages of the Wizard

If you have created a site and a machine catalog but not a delivery group, Web Studio guides you to the correct starting point to create one.

If you have already created a delivery group and want to create another, follow these steps:

1. Select **Delivery groups**.
2. In the action pane, select **Create Delivery Group**.
3. To organize delivery groups, you can create folders under the default **Delivery Groups** folder. For more information, see Create a folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select the folder where you want to create the group, then click **Create Delivery Group**. The group creation wizard opens.
5. The wizard starts with an **Introduction** page, which you can choose to skip in future launches. It then guides you through several pages, as described in the following table. After completing each page, click **Next** to proceed until you reach the final page.

	MULTI-SESSION OS	SINGLE-SESSION OS STATIC (ASSIGNED)	SINGLE-SESSION OS SHARED (POOLED)	REMOTE PC ACCESS
Pages	Machines	Machines	Machines	Machines
	Load Balancing	Delivery Type	Users	Users
	Users	Users	Applications	Applications
	Applications	Applications	Desktops	Desktop Assignment Rules
	Desktops	Desktop Assignment Rules	App Protection	App Protection
	App Protection	App Protection	Scopes	Scopes
	Scopes	Scopes	License agreement	License agreement
	License agreement	License agreement	Policy Set	Policy Set
	Policy Set	Policy Set	Local Host Cache	Summary
	Summary	Summary	Summary	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- You see the **Machine Allocation** page (just after the **Machines** page) if there is any available assigned machine in the selected single-session OS static machine catalog.
- The Local Host Cache mode page is available only for delivery groups containing power-managed single-session pooled machines.

Machines page

1. To create a delivery group with single-session suspend-capable only VMs, select **Make suspend capability required for this delivery group**.

   NOTE:

   This feature is applicable to only single-session suspend-capable machines.

2. Select a machine catalog and select the number of machines you want to use from that catalog.

Important considerations

- When choosing a catalog, the list only shows catalogs with at least one unused machine.
- A catalog can provide machines to more than one delivery group. A machine can be used in only one delivery group. When you add more machines to the delivery group, Web Studio suggests the same catalog by default.
- A delivery group can use machines from more than one catalog; however, those catalogs must contain the same machine types (multi-session OS, single-session OS, or Remote PC Access). All machines within a delivery group must have the same assignment type (pooled or static). In other words, you cannot mix machine types in a delivery group.
- Citrix® recommends using the latest VDA version on all machines.
- For **Remote PC Access**, when you create a site, a catalog named **Remote PC Access Machines** and a delivery group named **Remote PC Access Desktops** are created automatically. Each machine in a **Remote PC Access Machines** catalog is automatically associated with a delivery group.
- The following compatibility checks are performed:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- MinimumFunctionalLevel must be compatible
- SessionSupport must be compatible
- AllocationType must be compatible for SingleSession
- Remote PC Access is only compatible with Remote PC Access catalog

Machine Allocation page

The **Machine Allocation** page is available if there is any available assigned machine in the single-session OS static machine catalog selected on the **Machines** page.

Using this page, manage user assignments and desktop display names for machines in this delivery group.

- Use the **Display name** field to manage the desktop display name.
- Click **Browse** and select users or groups.

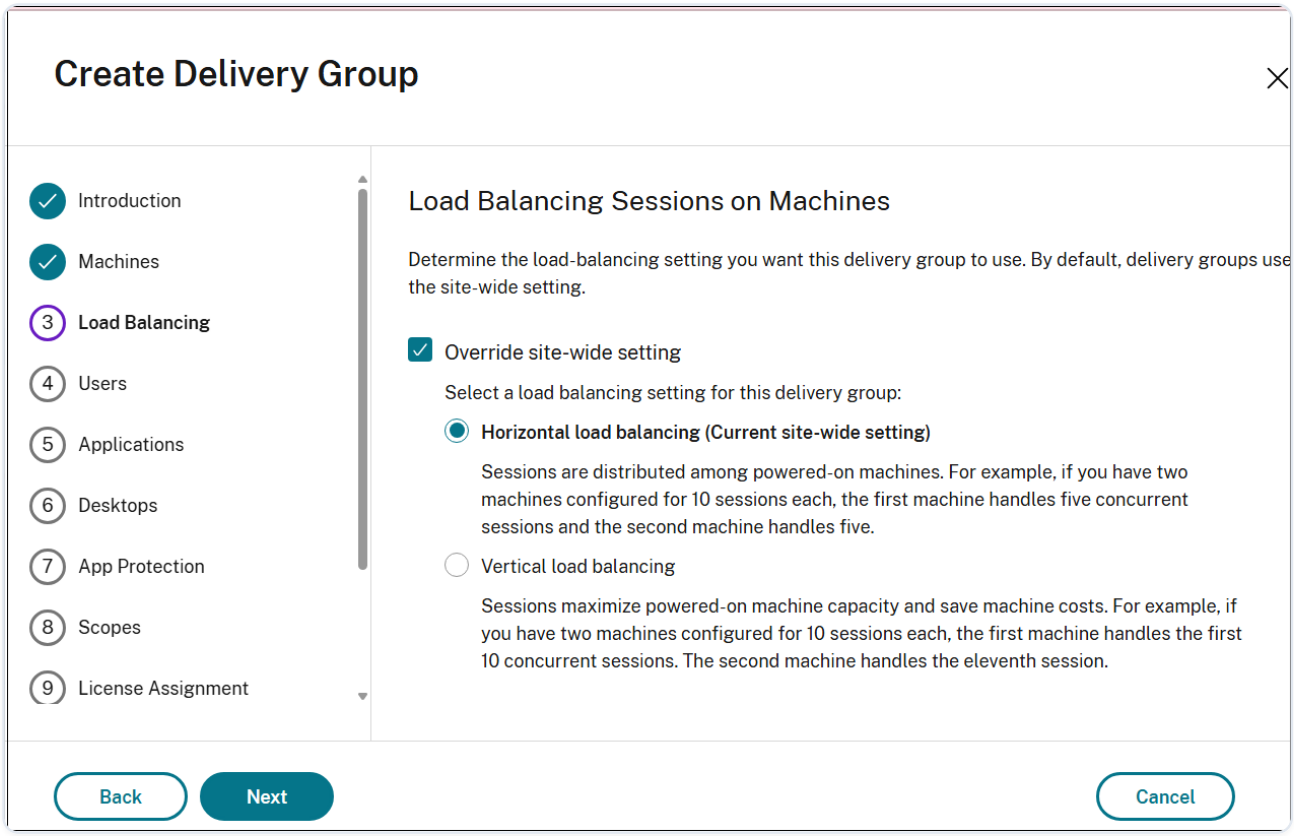
Load Balancing page

The **Load Balancing Sessions on Machines** page is available for multi-session OS machines.

Using this page, configure the load-balancing setting you want this delivery group to use. By default, delivery groups use the site-wide setting.

1. To configure a load balancing setting for this delivery group, select the **Override site-wide** setting checkbox.
2. Select either **Horizontal load balancing** or **Vertical load balancing** option as required. For information on Horizontal and Vertical load balancing methods, see Load balance machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If you select **Vertical load balancing**, make sure that the Concurrent logon tolerance and Maximum number of sessions policies are configured appropriately.

Delivery Type page

The **Delivery Type** page appears only for single-session OS static (assigned) machines.

Using this page, configure the machines in the catalog to deliver desktops or applications to your users.

1. Select either **Applications** or **Desktops.** You cannot enable both.

> **NOTE:**
>
> If you select machines from a multi-session OS or single-session OS random (pooled) catalog, the delivery type is assumed to be applications and desktops. You can deliver applications, desktops, or both.

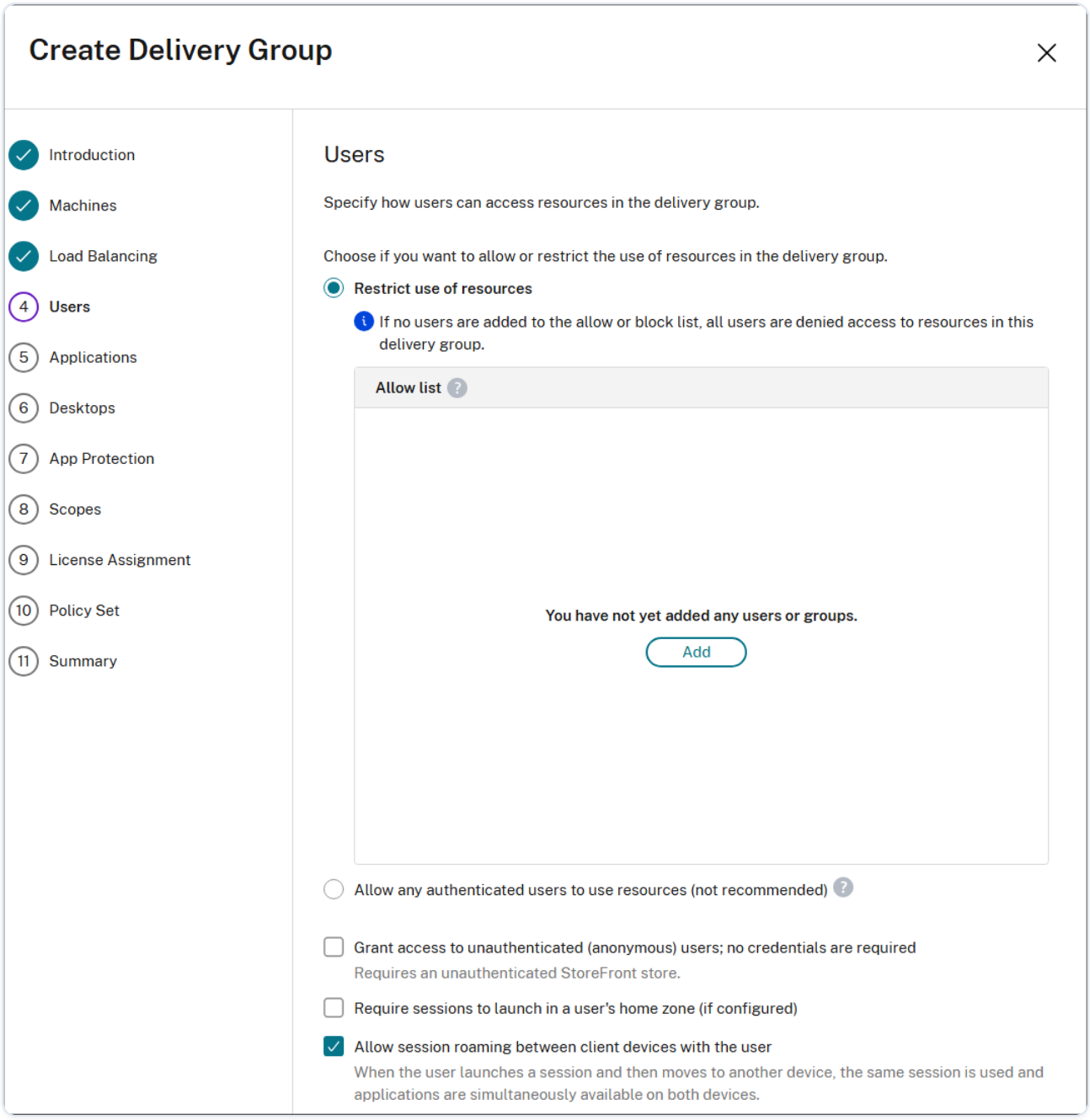
Users page

The **Users** page is available for all machine types. However, the options of the page vary with different types of machines.

Using this page, specify how users can access resources in the delivery group.

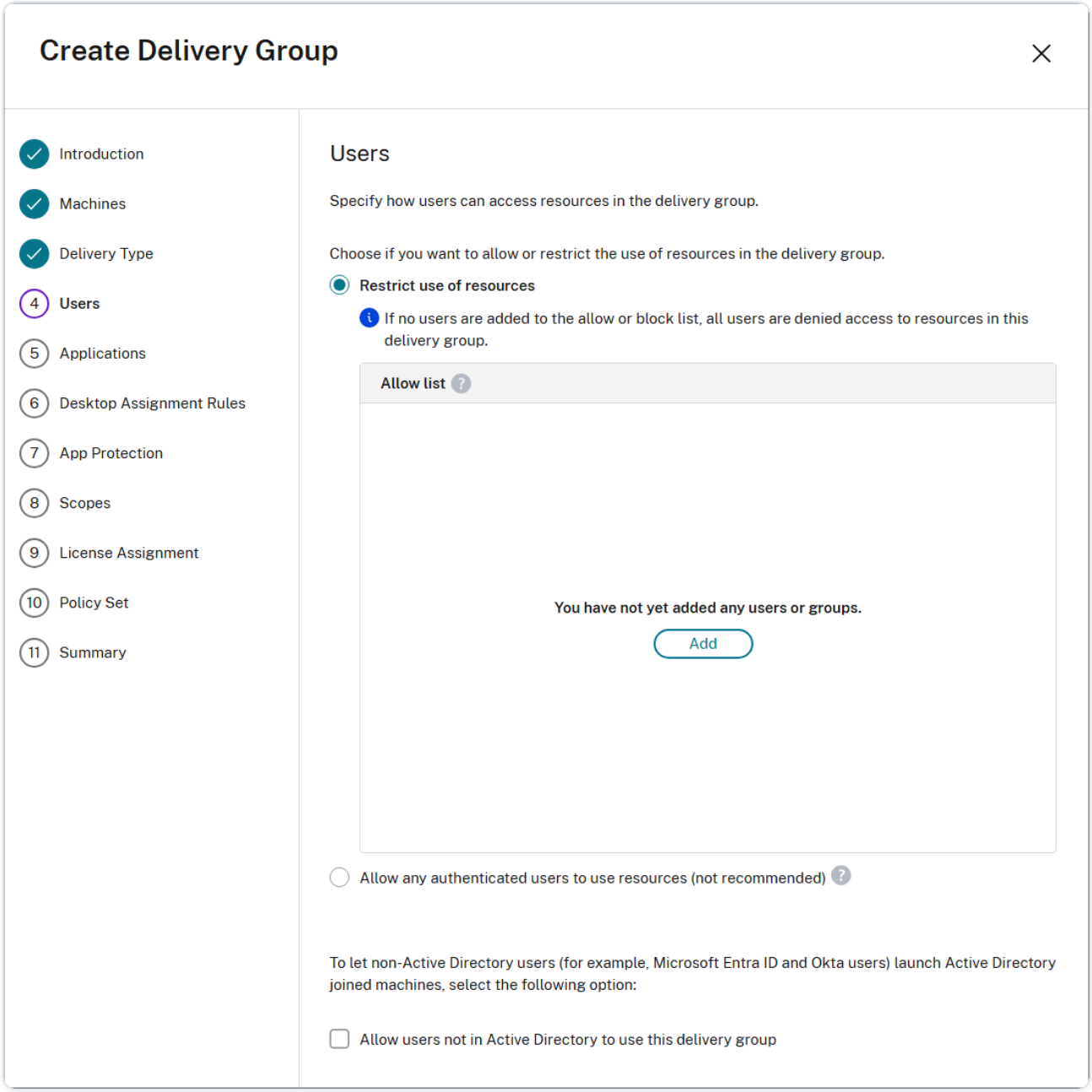
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For multi-session OS machines:



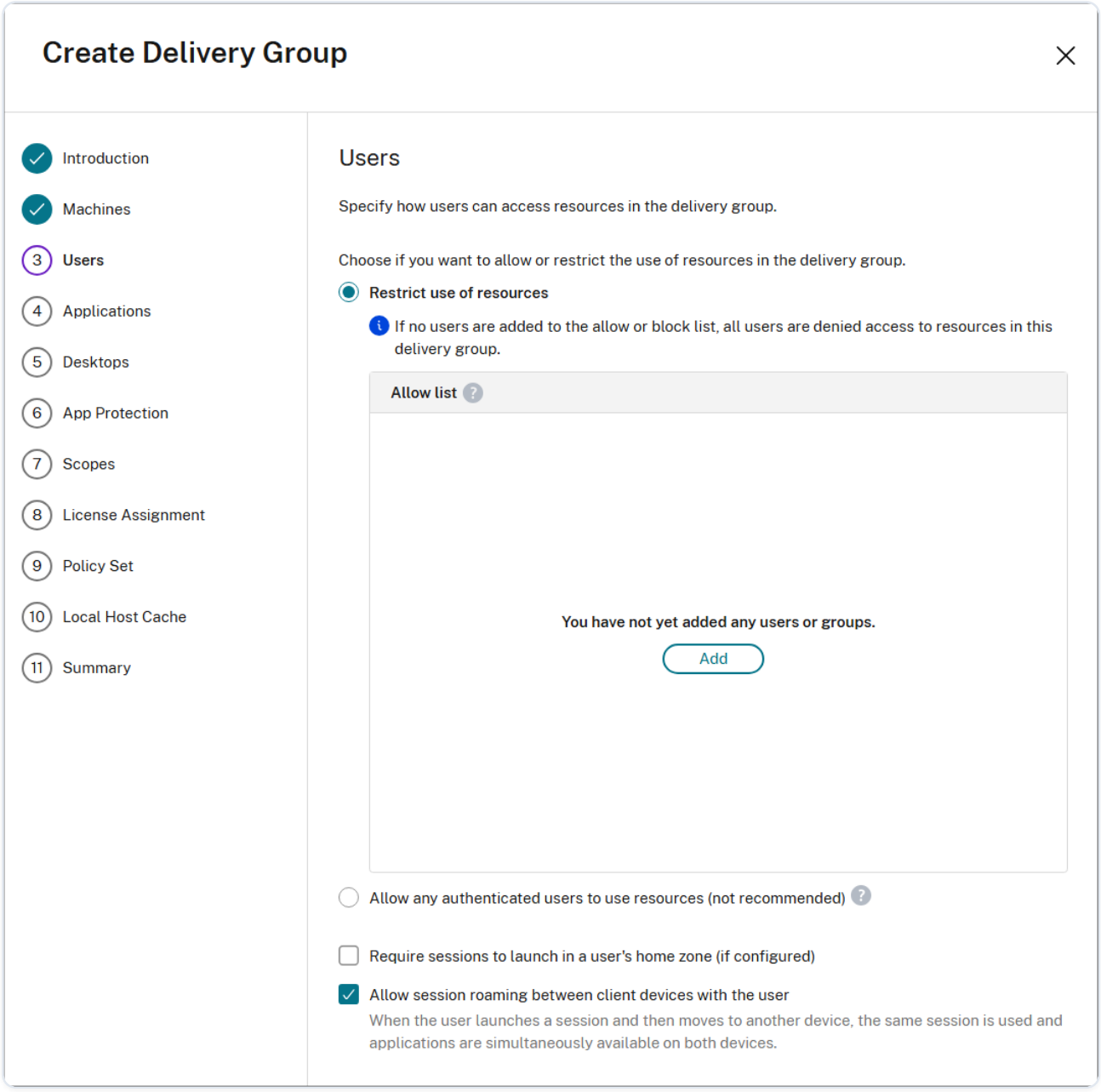
For single-session OS static machines:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For single-session OS shared machines:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



How user access control works

User access in a delivery group is controlled through specified user lists when you create or edit access settings.

- Users who meet *all* of the following conditions can access **applications** in a delivery group:
  - Have access to resources (apps and desktops) in this delivery group. By default, access is determined by the deployment's user access list (users in the Active Directory), which is not configured through Studio. See Add or remove users in a delivery group.
  - Have access to applications in this group. By default, the application entitlement policy rule includes everyone. See the PowerShell SDK `BrokerAppEntitlementPolicyRule`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

cmdlets for details. If needed, you can restrict user access to applications in a delivery group using **Delivery Groups > Edit Application Assignment Rule**.

- Have access to application groups that include this application.

- Users who meet *both* of the following conditions can access desktops in a delivery group:
  - Have access to resources (apps and desktops) in this delivery group. By default, access is determined by the deployment's user access list (users in the Active Directory), which is not configured through Studio. You can add or remove users from the default user scope. See Add or remove users in a delivery group.
  - Have access to desktops in this group. For more information, see Desktops (or Desktop Assignment Rules page).

NOTE:

- When specifying a user or group list, you can select accounts from any connected identity types, including Active Directory, Microsoft Entra ID, or Okta. Additionally, you can select accounts from multiple providers of the same identity type.

Configuration steps

1. Select one of the options to allow or restrict the use of resources in the delivery group.
   - **Allow any authenticated users to use resources:** To access applications and desktops, the users and group members you specify by name must present credentials such as smart card or user name and password to StoreFront™ or Citrix Workspace™ app. (For delivery groups containing single-session OS machines, you can import user data (a list of users) later by editing the delivery group.)
   - **Restrict use of resources:** Alternatively, you can restrict use of a delivery group by adding users or user groups to the **Allow list**. Only users on the **Allow list** can access apps and desktops in the delivery group. You can also add users and user groups to a block list by clicking **Add block list**, which prevents users from using apps and desktops in the selected delivery group. A block list is meaningful only when used to block users in the allow list.
2. For multi-session OS machines, select **Grant access to unauthenticated (anonymous) users; no credentials are required** if you want users to access applications and desktops without presenting credentials to StoreFront or Citrix Workspace app. For example, at kiosks, the application might require credentials, but the Citrix access portal and tools do not.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Unauthenticated user accounts are created on demand when a session is launched, and named AnonXYZ, in which XYZ is a unique three-digit value.
- Unauthenticated user sessions have a default idle timeout of 10 minutes, and are logged off automatically when the client disconnects. Reconnection, roaming between clients, and Workspace Control are not supported.

3. Select **Require sessions to launch in a user's home zone (if configured**) to prevent sessions from defaulting to other available zones if the user's home zone has sufficient resources.
4. Select **Allow session roaming between client devices with the user** if you want the sessions to follow, regardless of the device or whether current sessions exist.See Session roaming.
5. To enable non-Active Directory users to launch sessions on machines using a local account, select **Allow users not in Active Directory to use this delivery group** checkbox. This action facilitates the automatic creation and mapping of a local Windows account to the logged-in user. Consequently, all logins for this delivery group will use a mapped local account on the VDAs for log in. While allowing non-Active Directory users to access a local account on the VDA is one use case, this functionality also extends to Active Directory logins.

   NOTE:

   If the user's Azure UPN contains a dot as the twentieth character, the Windows Server VDA is unable to create a local user account.

The following table describes your choices on the **Users** page:

ENABLE ACCESS FOR	ADD/ASSIGN USERS AND USER GROUPS?	ENABLE THE “GIVE ACCESS TO UNAUTHENTICATED USERS” CHECKBOX?
Only authenticated users	Yes	No
Only unauthenticated users	No	Yes
Both authenticated and unauthenticated users	Yes	Yes

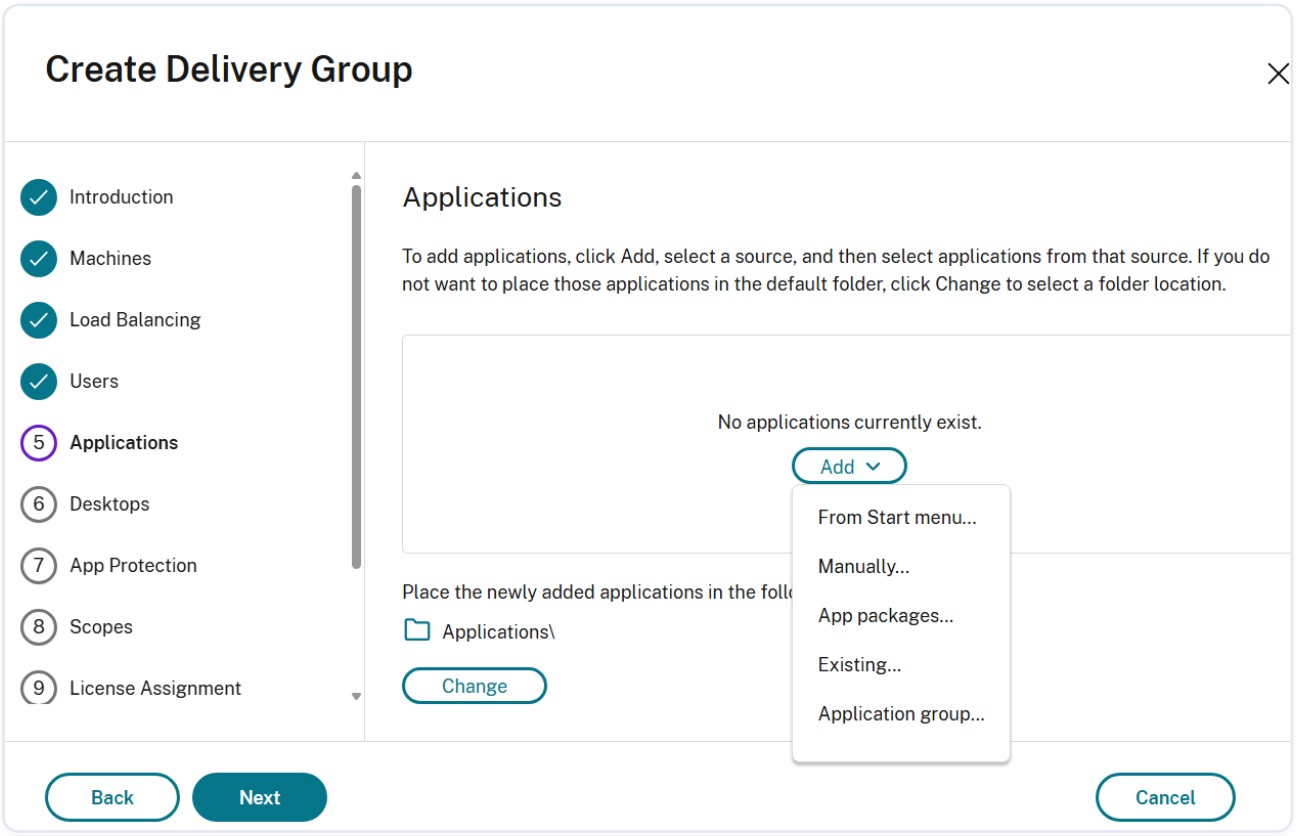
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications page

The **Applications** page is available for all machine types. However, the applications that you can add vary with different types of machines.

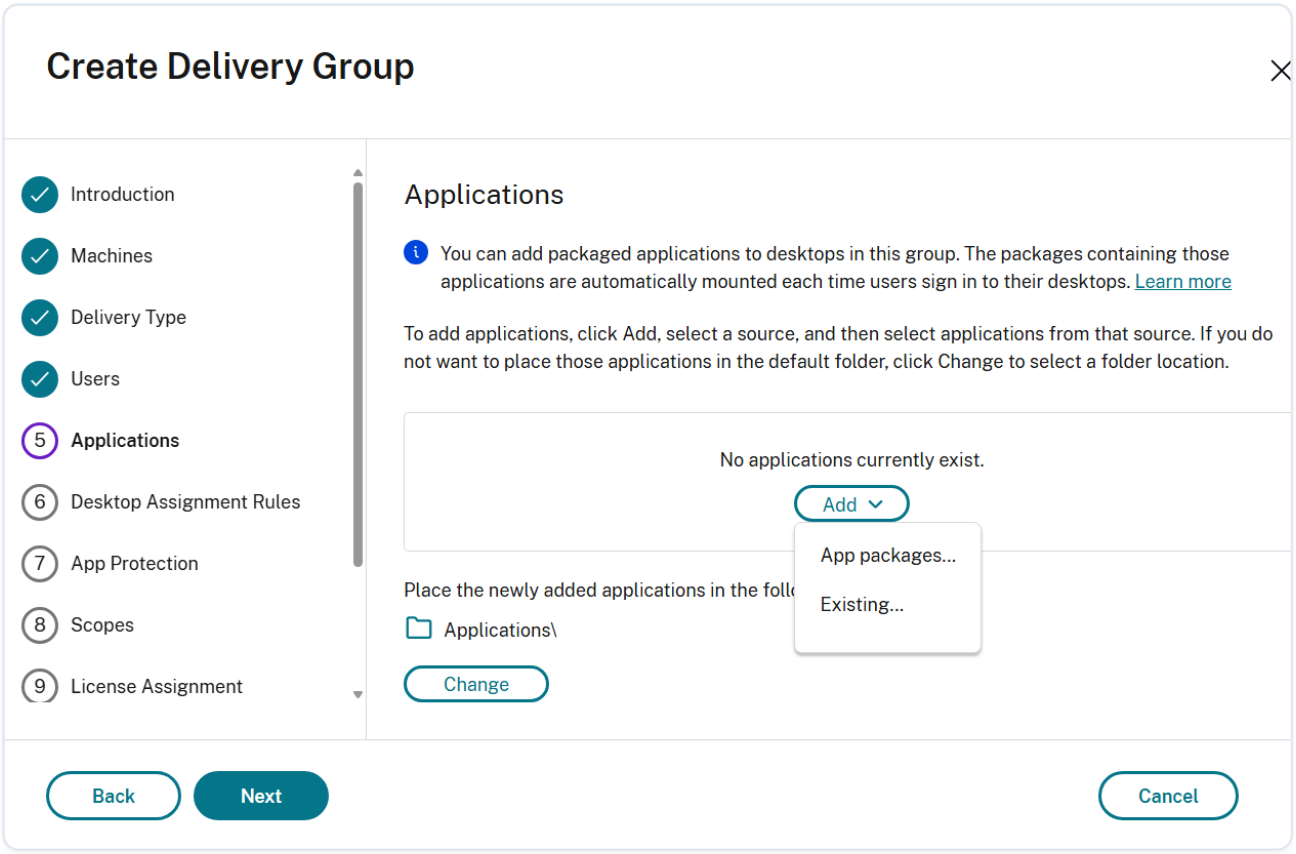
Using this page you can add packaged applications to desktops in this group.

For multi-session and single-session shared OS machines:



For single-session static OS machines:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Important considerations

- You can add packaged applications to delivery groups. The packages containing those applications are automatically mounted each time users sign in to their desktops or Remote PCs.
- By default, new applications you add are placed in a folder named Applications. You can specify a different folder. For details, see the Applications article.
- You can change the properties for an application when you add it to a delivery group, or later. For details, see the Applications article.
- If you try to add an application and one with the same name exists in that folder, you are prompted to rename the application you are adding. If you decline, the application is added with a suffix that makes it unique within that application folder.
- When you add an application to more than one delivery group, a visibility issue can occur if you do not have permission to view the application in all those delivery groups. In such cases, either consult an administrator with greater permissions or have your scope extended to include all the delivery groups to which the application was added.
- If you publish two applications with the same name to the same users, change the Application name (for user) property. Otherwise, users see duplicate names in the Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration steps

1. Select the **Add** menu to display the application sources.

    - **From Start menu:** Applications are discovered through one of the currently registered VDAs that are assigned to the delivery group. When you select this source, a new page launches with a list of discovered applications; select those you want to add and then select **OK**.
    - **Manually:** Applications located in the deployment or elsewhere in your network. When you select this source, a new page launches where you type the path to the executable, working directory, optional command line arguments, and display names for administrators and users. After entering this information, select **OK**.
    - **Existing:** Applications previously added to the deployment, perhaps in another delivery group. When you select this source, a new page launches with a list of discovered applications; select those you want to add and then select **OK**.
    - **Application packages:** Applications in App-V, MSIX, MSIX app attach, or FlexApp application packages. When you select this source, the **Add Applications from Packages** page launches. Select an application package source, select the applications you want to add from the resulting display, and then select **OK**.

        NOTE:

        ◦ This option is dimmed if no application package is configured for the site.

        \> - To publish MSIX or MSIX app attach apps, the delivery group's functional level must be 2106 or later. For FlexApp apps, the functional level must be 2206 or later. When a functional level requirement isn't met, the corresponding options in the **Application package source** drop-down list are dimmed.

- **Application group:** Application groups that exist in the deployment.

If an application source or application is not available or valid, it is either not visible or cannot be selected. For example, the **Existing** source is not available if no applications have been added to the deployment. Or, an application might not be compatible with the supported session types on machines in the selected machine catalog.

Desktops (or Desktop Assignment Rules) page

The title of this page depends on the machine catalog that you chose earlier in the wizard:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you choose a catalog containing multi-session or pooled single-session machines, this page is titled **Desktops**.
- If you choose a catalog containing single-session static machines and specified “Desktops” on the **Delivery Type** page, this page is titled **Desktop Assignment Rules**.

> **NOTE:**
>
> - If you choose a catalog containing single-session static machines and specified “Applications” on the **Delivery Type** page, then you do not see the page.

1. (Optional) To update the default desktop icon for the delivery group, select **Change**. You can extract the icon from an `.ico` file or an `.exe` file. The maximum supported icon file size is 500 KB. This icon applies to all desktops in the group unless a different icon is set for an individual desktop.
2. Select **Add**. In the dialog box:

    a. In the **Display name** and **Description** fields, type the information to be displayed in the Citrix Workspace app.

    b. For multi-session or pooled single-session OS machines: To add a tag restriction to a desktop, select **Restrict launches to machines with this tag** and then select the tag from the menu.

    c. Using the radio buttons, you can either:

        i. **Allow everyone with access to this delivery group to use a desktop.** All users in the delivery group can launch a desktop (for groups with pooled machines) or be assigned a machine when they launch the desktop (for groups with single-session static machines).

        ii. **Restrict desktop use** by adding users and user groups to the **Allow list**. Only users on the **Allow list** can access a desktop. You can also add users and user groups to a block list by clicking **Add block list**, which prevents users from using desktops in the selected delivery group. A block list is meaningful only when used to block users in the allow list.

    d. If the group contains single-session static machines, specify the maximum number of desktops per user. This must be a value of one or greater. The setting is not mandatory. You can assign machines manually or use RemotePC to have the machines assigned automatically.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. (Optional) Select **Change** to update the desktop icon for pooled desktops or the desktop assignment rule for single-session static desktops. You can browse to select an icon from an `.ico` or an `.exe` file.The specified icon overrides the default icon set at the delivery group level.

f. Enable or disable the desktop (for multi-session machines) or desktop assignment rule (for single-session static machines): Disabling a desktop stops desktop delivery. Disabling a desktop assignment rule stops desktop auto-assignment to users.

g. When you are finished with the dialog box, select **OK**.

App Protection page

The **App Protection** page is available for all machine types.

Using this page, you provide enhanced security for Citrix published apps and desktops.

The following information is supplemental to the App protection article in the Citrix Virtual Apps and Desktops documentation. To use app protection in a Citrix DaaS deployment, follow the general guidance in that article, minding the following details.

- You must have a valid Citrix Cloud™ subscription and valid app protection entitlements. To purchase the app protection feature, you can contact your Citrix sales representative. (For on-premises: You must have a valid App Protection entitlement. To purchase the App Protection feature, contact your Citrix sales representative.)
- App protection requires XML trust. To enable XML trust, go to **Settings > Site settings > Enable XML trust**.

Protection is applied under the following conditions:

- **Anti-screen capture**:
  - On Windows and macOS, only the window of the protected content is blank. App protection is active when a protected window is not minimized.
  - On Linux, the entire capture is blank. App protection is active whether a protected window is minimized or not.
- **Anti-keylogging**: Enabled if a protected window is in focus. To disable protection, change focus to another window.

Scopes page

The **Scopes** page is available for all machine types.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using this page, group objects (for example, connections, catalogs, and delivery groups) in a way that is relevant to your organization.

License assignment page

The **License assignment** page is available for all machine types.

Using this page, specify which license you want the delivery group to use. By default, the delivery group uses the site license. For more information, see Licenses.

Policy Set page

The **Policy Set** page is available for all machine types.

Using this page, specify which policy set you want this delivery group to use.

Local Host Cache mode page

This page is available only for delivery groups containing power-managed single-session pooled machines.

By default, pooled machines that are power managed can be used for only one session when in Local Host Cache (LHC) mode. To change the default behavior and make them always available for new user connections when in LHC mode, select **Use machines for subsequent sessions**.

Alternatively, you can change the default behavior using PowerShell commands. For more information, see Application and desktop support.

IMPORTANT:

Enabling access to power-managed single-session pooled machines can cause data and changes from previous user sessions being present in subsequent sessions.

One-time use pooled desktops in Local Host Cache

During a Local Host Cache (LHC) outage, pooled desktops can be used on a one-time basis. This is achieved by issuing a hygiene blob to capable VDAs and initiating reboots. This process guarantees a clean state for the desktops upon recovery from the outage. For machines that are not capable or legacy, participation only occurs if reuse is explicitly enabled. The feature improves customer sentiment during outages by making availability more seamless.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

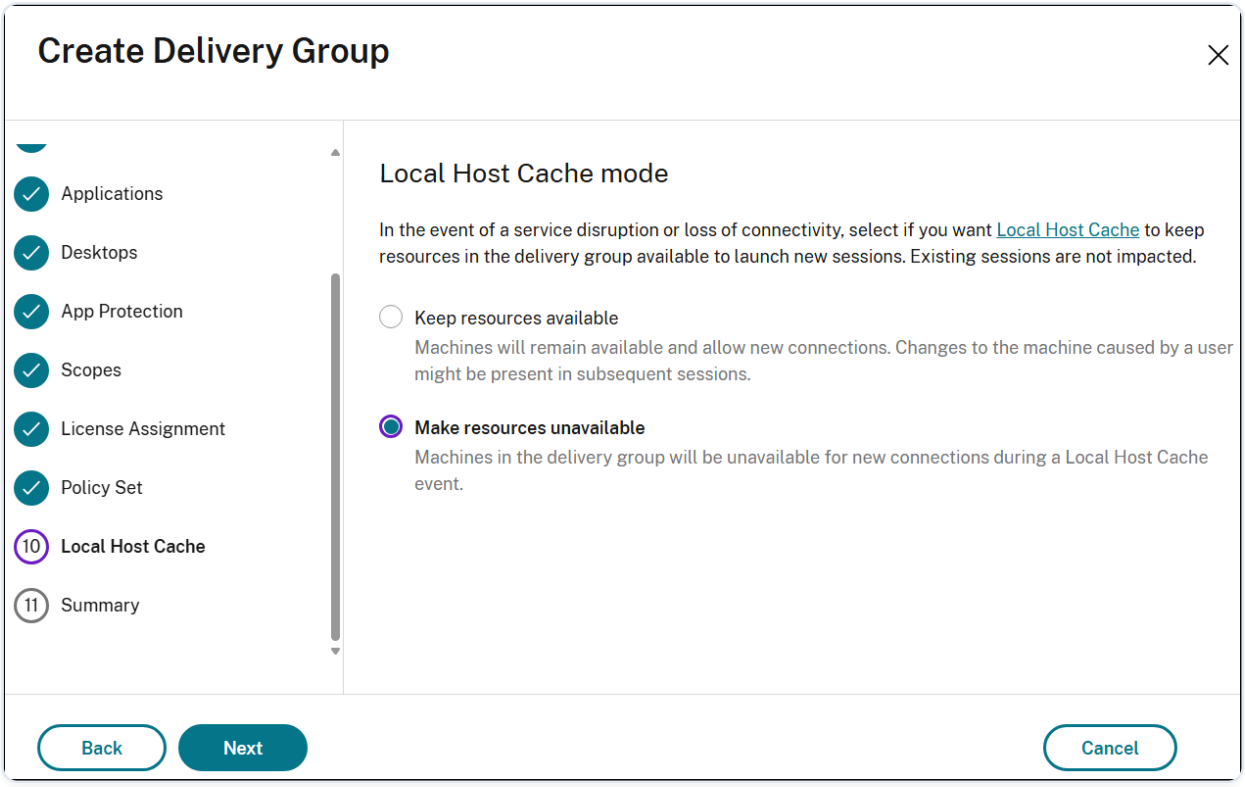
Prerequisites

- VDA version 2407 or later for full hygiene enforcement. Legacy VDAs (prior to VDA version 2407) can be used only when reuse is enabled. These VDAs do not receive the hygiene blob or enforced reboots.
- Machine catalogs with single session machines.

Configure one-time use of pooled desktops

1. Create an MCS catalog with single session machines using VDA build 2407 or greater.
2. Create a corresponding delivery group. Set the `ReuseMachinesWithoutShutdownInOutage` desktop group setting to `false` for the delivery group from Remote PowerShell or select **Make resources unavailable** in Studio on the **Local Host Cache mode** page when creating a delivery group.

   ```
   Set-BrokerDesktopGroup -Name "name"
   -ReuseMachinesWithoutShutdownInOutage $false
   ```

3. After you complete the configuration, during LHC outage mode, machines are available for one-time use. When out of LHC outage mode, machines that were tainted are rebooted and available to be used again.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

A machine is classified as tainted once a user session has been initiated following its most recent power-on. An untainted machine refers to a machine that has not launched any user sessions since its latest power-on event.

Summary page

Enter a name for the delivery group. You can also (optionally) enter a description, which appears in the Citrix Workspace app and in Studio.

Review the summary information and then click **Finish**.

Limitation

Assignment of a desktop to a client IP address only works with a limited set of client types and configurations. Performing access filtering based on the client IP address uses the public IP address for cloud clients.

More information

- Manage delivery groups
- Applications

Manage delivery groups

Introduction

This article describes procedures for managing delivery groups from the management console. In addition to changing the settings specified when creating the group, you can configure other settings that are not available when you create a delivery group.

The procedures are organized according to the categories: general, users, machines, and sessions. Some tasks span more than one category. For example, "Prevent users from connecting to machines" is described in the machines category, but it also affects users. So, if you can't find a task in one category, check a related category.

Other articles also contain related information:

- Applications contain information about managing applications in delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Managing delivery groups requires the Delivery Group Administrator built-in role permissions. For details, see Delegated administration.

General

- View group details
- Change preferred properties
- Change the delivery type
- Change StoreFront™ addresses
- Change the functional level
- Manage Remote PC Access delivery groups
- Change the license for a delivery group
- Organize delivery groups using folders
- Manage app protection
- Change suspend capability for a delivery group

View group details

1. Use the search function to locate a specific delivery group. Refer to Search for instances for instructions.
2. From the search results, select a group as necessary.
3. Refer to the following table for descriptions of the group columns.
4. Click a tab in the bottom details pane for more information about this group.

COLUMN	DESCRIPTION
Delivery Group	The group name and the session type. Session types include Single-session OS and Multi-session OS.
Delivering	The type of resources delivered from this group. Possible values include Applications, Desktops, and Applications and Desktops. "Static machine assignment" appears if the delivery group consists of dedicated machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION
Session in Use	The number of machines that are set up and the number of machines that are in a Disconnected state.
Allocated Count	The number of machines in the catalog assigned to a delivery group.
Folder	The location of the group within the **Delivery Groups** tree. It displays the name of the folder that the group is in (including the trailing backslash), or `-` if the group is at the root level.

Change preferred properties

Preferred properties control how users access and launch resources from a delivery group. To change preferred properties for a delivery group, follow these steps:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Preferences** page, change any of the settings in the following table.
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

SETTING	DESCRIPTION
Description	The text that end users see.
Enable Delivery Group	Whether the delivery group is enabled.
Time zone	The time zone in which the machines of this delivery group reside. This setting automatically shows the time zone set in **Settings > Date and Time** for a newly created delivery group. You can choose a different time zone for the delivery group if

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SETTING	DESCRIPTION	
	needed. The drop-down menu lists the time zones supported by the site. **Note:** Changing the time zone on a delivery group might reboot the machines in that delivery group. To avoid this, ensure to change the time zone settings outside of production hours.	
Enable Secure ICA®	Secures communications to and from machines in the delivery group using SecureICA, which encrypts the ICA protocol. The default level is 128-bit. The level can be changed using the SDK. Citrix® recommends using more encryption methods such as TLS encryption when traversing public networks. Also, SecureICA does not check data integrity.	

Change the delivery type of a delivery group

The delivery type indicates what the group can deliver: applications, desktops, or both.

Before changing an **applications** type to the **Desktops** type, delete all applications from the group.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Delivery Type** page, select the delivery type you want.
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change StoreFront addresses

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **StoreFront** page, indicate whether you will specify a StoreFront server address later (**Manually**) or select **Add new** to specify the StoreFront servers you want to be used (**Automatically**).
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

You can also specify StoreFront server addresses from the **Settings** tab within the **Delivery Groups** node.

Change the functional level

Change the functional level for the delivery group after you upgrade the VDAs on its machines and the machine catalogs containing the machines used in the delivery group.

Before you start:

- If you use Citrix Provisioning™ (formerly Provisioning Services), upgrade the VDA version in the Citrix Provisioning console.
- Start the machines containing the upgraded VDA so that they can register with Citrix DaaS. This process tells the console about what must change in the delivery group.
- If you must continue to use earlier VDA versions, newer product features might not be available. For more information, see the upgrade documentation.

To change the functional level for a delivery group:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Change Functional Level** in the action bar. The **Change Functional Level** action appears only if upgraded VDAs are detected.

The display indicates you which, if any, machines cannot be changed to the functional level and why. You can then cancel the change action, resolve the machine issues, and then perform the change action again.

After the change completes, you can revert the machines to their previous states. Select the delivery group and then select **Undo Functional Level Change** in the action bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage Remote PC Access delivery groups

If a machine in a Remote PC Access machine catalog is not assigned to a user, the machine is temporarily assigned to a delivery group associated with that catalog. This temporary assignment enables the machine to be assigned to a user later.

The delivery group-to-machine catalog association has a priority value. Priority determines which delivery group that machine is assigned to when it registers with the system or when a user needs a machine assignment: the lower the value, the higher the priority. If a Remote PC Access machine catalog has multiple delivery group assignments, the software selects the match with the highest priority. Use the PowerShell SDK to set this priority value.

When first created, Remote PC Access machine catalogs are associated with a delivery group. This association means that machine accounts or Organizational Units added to the catalog later can be added to the delivery group. This association can be switched off or on.

To add or remove a Remote PC Access machine catalog association with a delivery group:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a Remote PC Access group.
3. In the **Details** section, select the **Machine Catalogs** tab and then select a Remote PC Access catalog.
4. To add or restore an association, select **Add Desktops**. To remove an association, select **Remove Association**.

Change the license for a delivery group

To change the license entitlement for a delivery group, follow these steps:

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **License Assignment** page, select the license you want the group to use.
4. Click **Apply** to apply any changes you made and to keep the window open. Or, click **Save** to apply changes and to close the window.

For more information about delivery group-level entitlements, see Licenses.

Organize delivery groups using folders

Create folders to organize delivery groups for easy access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP:

You can set your preferred default view (folder or list view) for the Delivery Groups node by clicking the **Folder** icon on the top right of the action bar.

Required roles

By default, you need to have the following built-in role to create and manage delivery group folders: Cloud Administrator, Full Administrator, or Delivery Group Administrator. If necessary, you can customize roles for creating and managing delivery group folders. For more information, see Required permissions.

Create a delivery group folder

Before you start, plan how to organize your delivery groups. Consider the following:

- You can nest folders up to five levels (*excluding* the default node folder).
- A folder can contain delivery groups and subfolders.
- All nodes in Studio (such as **Machine Catalogs**, **Delivery Groups**, **Applications**, and **Application Groups**) share the same folder tree in the back end. To avoid name conflicts when renaming or moving folders, use unique names for first-level folders across different nodes.

  If you create a folder using the `New-BrokerAdminFolder` SDK cmdlet and want it to appear under the **Delivery Groups** node, you must add the `ContainsDeliveryGroups` metadata using the `Set-BrokerAdminFolderMetadata` cmdlet.

  Example:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsDeliveryGroups -Value true
  ```

To create a delivery group folder, follow these steps:

1. From Studio, select **Delivery Groups** in the left pane.
2. In the folder hierarchy, select a folder and then select **Create Folder** in the **Action** bar.
3. Enter a name for the new folder, and then click **Done**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP:

If you create a folder in an unintended location, you can drag it to the correct location.

Move a delivery group

You can move a delivery group between folders. Detailed steps are as follows:

1. From Studio, select **Delivery Groups** in the left pane.
2. View groups by folder. You can also turn on **View all** above the folder hierarchy to view all groups at a time.
3. Right-click a group and then select **Move Delivery Group**.
4. Select the folder to which you want to move the group, and then click **Done**.

TIP:

You can drag a group to a folder.

Manage delivery group folders

You can delete, rename, and move delivery group folders.

You can delete a folder only if it and its subfolders don't contain delivery groups.

To manage a folder, follow these steps:

1. From Studio, select **Delivery Groups** in the left pane.
2. In the folder hierarchy, select a folder, and then select an action in the **Action** bar as needed:
   - To rename the folder, select **Rename Folder**.
   - To delete the folder, select **Delete Folder**.
   - To move the folder, select **Move Folder**.
3. Follow the onscreen instructions to complete the remaining steps.

Required permissions

The following table lists the permissions required to perform actions on delivery group folders.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	REQUIRED PERMISSIONS
Create delivery group folders	Create Delivery Group Folder
Delete delivery group folders	Remove Delivery Group Folder
Move delivery group folders	Move Delivery Group Folder
Rename delivery group folders	Edit Delivery Group Folder
Move delivery groups to folders	Edit Delivery Group Folder and Edit Delivery Group Properties

Manage app protection

The following information is supplemental to the App protection article in the Citrix Virtual Apps and Desktops documentation. To use app protection in a Citrix DaaS deployment, follow the general guidance in that article, minding the following details.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **App Protection** page, you can see the following options:

OPTIONS	DESCRIPTION
Do not apply	Select this option to not apply the setting.
Apply to this delivery group	Select **Anti-keylogging** and/or **Anti key capturing** options. Hover over each of these settings to read the details in the tool tip.
Apply contextually	To apply this setting, configure the access policy in the **Access Policy settings** page.
	1. Click **Access Policy** in the left pane and click **Add**.
	1. On the **Add Policy** page, do the following
	- i. Enter a **Policy name** and configure the settings as required.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTIONS	DESCRIPTION
	- ii. In the **Filter** and **Value** fields, enter the details and click **Done**. The new policy is listed in the **App Protection** page. Enable the required settings for this policy.
	- iii. Click **Save**.

4. On the **Delivery Group** page, select the **Delivery Group** and click the **Details** tab at the bottom. The new **App Protection** settings applied are displayed.

- You must have a valid Citrix Cloud™ subscription and valid app protection entitlements. To purchase the app protection feature, you can contact your Citrix sales representative.
- App protection requires XML trust. To enable XML trust, go to **Settings > Site settings > Enable XML trust**.
- Regarding anti-screen-capturing:
  - On Windows and macOS, only the window of the protected content is blank. App protection is active when a protected window is not minimized.
  - On Linux, the entire capture is blank. App protection is active whether a protected window is minimized or not.

Change suspend capability for a delivery group

Make the suspend capability required or optional for a delivery group:

- **Required**: The delivery group can only include those VMs that are suspend capable.
- **Optional**: The delivery group can include VMs that are or aren't suspend capable.

Before you begin

You can only change the suspend-capability of a delivery group to `Required` if all the VMs present in the delivery group are suspend-capable.

To change the suspend-capability of a delivery group:

1. From Studio, go to **Delivery Groups** in the left pane.
2. Select a group, and then click **Change Suspend Capability** in the action bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Users

NOTE:

The option **Leave user management to Citrix Cloud** has been removed. To manage user assignments for existing delivery groups set to **Leave user management to Citrix Cloud**, see Manage user assignments for Citrix Cloud Library-managed delivery groups.

This topic covers the following sections:

- Add or remove users
- Manage user assignments for Citrix Cloud Library-managed delivery groups
- Restrict user access to desktops and apps in a delivery group
- Restrict user access to resources in a delivery group
- Restrict user access to resources across all delivery groups
- Configure user scope for an access policy

Add or remove users in a delivery group

For detailed information about users, see Users.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit Delivery Group** in the action bar.
3. On the **Users** page:
    - To add users, select **Add**, and then specify the users you want to add.
    - To remove users, select one or more users and then select **Remove**.
    - Select or clear the check box to allow access by unauthenticated users.
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

Manage user assignments for Citrix Cloud Library-managed delivery groups

For Citrix Cloud Library-managed delivery groups, you can manage their user assignments using Full Configuration. Detailed steps are as follows:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a Citrix Cloud Library-managed delivery group, and then select **Edit** in the action bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. To restrict the use of a desktop to certain users, follow these steps:

    a. On the **Desktops** or **Desktop Assignment Rules** page, select the desktop and click **Edit**. The **Edit Desktop** page appears with the **Restrict desktop use** option selected.

    b. Click **Add**, select users as needed, and then click **Done**.

    c. Click **OK**.

4. To restrict the use of applications in this group to certain users, click **Application Assignment Rule**, and follow the similar steps described in step 3 to add users.

Restrict access to desktops and apps in a delivery group

You can manage user access to resources in a delivery group by performing the following tasks:

- Restrict desktop access to specific users
- Restrict application access to specific users

Restrict desktop access to specific users

Users who meet *both* of the following conditions can access desktops in a delivery group:

- Have access to resources (apps and desktops) in this delivery group.

  By default, access is determined by the deployment's user access list, which is not configured through Studio. You can add or remove users from the default user scope. See Add or remove users in a delivery group.

- Have access to desktops in this group.

  For more information, see Desktops (or Desktop Assignment Rules) page.

To restrict access to a desktop to specific users, see Desktops (or Desktop Assignment Rules) page.

Restrict application access to specific users

Users who meet *all* of the following conditions can access applications in a delivery group:

- Have access to resources (apps and desktops) in this delivery group.

  By default, access is determined by the deployment's user access list, which is not configured through Studio. You can add or remove users from the default user scope. See Add or remove users in a delivery group.

- Have access to applications in this group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, the application entitlement policy rule includes everyone. See the PowerShell SDK `BrokerAppEntitlementPolicyRule` cmdlets for details. If needed, you can restrict user access to applications in a delivery group using the steps described below.

- Have access to application groups that include this application.

To restrict application access to specific users at the delivery group level, follow these steps:

1. In Studio, select **Delivery Groups** in the left pane.
2. Select a delivery group, and then select **Edit** in the action bar.
3. To restrict application access, follow these steps:
   a. In the left pane, click the **Application Assignment Rule**.
   b. To allow specific users to access applications, select **Restrict application use**, and then click **Add** in the **Allow list** area and specify users or user groups to include.
   c. To block specific users from accessing applications, click **Add** in the **Block list** area and specify the users or user groups to exclude.

NOTE:

- If you select **Restrict application use** but leave both the Allow and Block lists empty, no users can use applications in this group.
- If you select **Restrict application use** and leave the Allow list empty, all users except users in the **Block list** can use the applications.

Restrict access to resources in a delivery group

Any changes you make to restrict access to resources in a delivery group supersede previous settings, regardless of the method you use. You can:

- **Restrict access for administrators using delegated administration scopes:** You can create and assign a scope that permits administrators to access all applications and another scope that provides access to only certain applications. For details, see Delegated administration.
- **Restrict access for users through smart access policy expressions:** You can configure access policy rules to control user access to a specific delivery group. Examples include:
  - Restrict access to a subset of users and specify allowed user devices.
  - Restrict access to users connected through cloud stores (instead of on-premises stores).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Restrict access to users connected through a specific store URL.

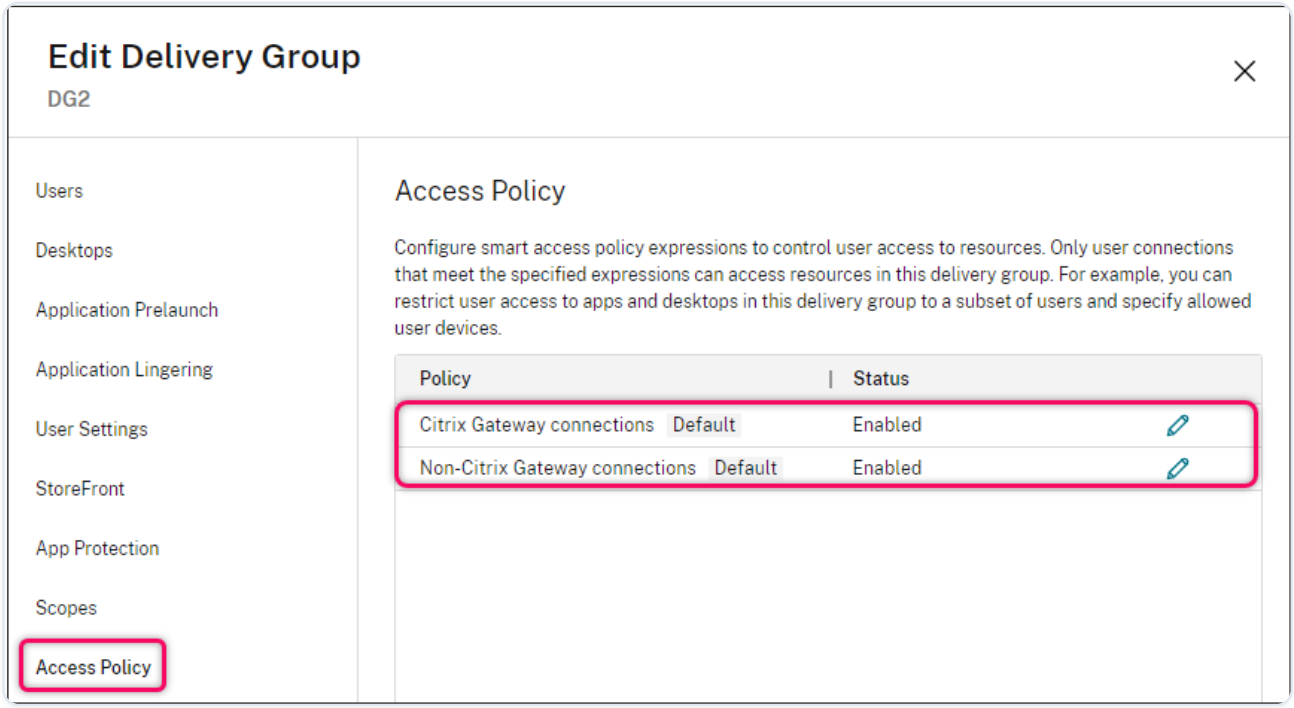
This section guides you through how to restrict user access to delivery groups through access policy rules:

- About access policy rules
- Add access policy rules
- Manage access policy rules using Studio
- Add and refine policy rules using PowerShell

About access policy rules

You can configure multiple access policy rules for a delivery group. Apps and desktops in a delivery group appear in a user's StoreFront or Workspace when the user's connection matches any access policy rule you defined for the delivery group, irrespective of order.

Each rule can be individually enabled or disabled. A disabled rule is ignored when the access policy is evaluated.



In Studio, the Access Policy list includes the following default SmartAccess policy rules. You can add more as necessary.

- **Citrix Gateway connections.** This policy allows only user connections made through Citrix Gateway can access resources within the delivery group. User connections made through Workspace when either the Device Posture or Network Location features are enabled, are also considered connections through Citrix Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Non-Citrix Gateway connections.** This policy allows only user connections made not through Citrix Gateway can access resources within the delivery group.

NOTE:

- To prevent the default rules from overriding a newly configured one, you must either disable the default rules or refine them to exclude the filters used in the new policy.
- The default policies can't be deleted but they can be disabled. To disable a policy, click the **Edit** icon and then change the **Policy state** to **Disabled**.
- The policy list also shows rules added using PowerShell commands. Those policies can be deleted but can’t be edited in Studio.

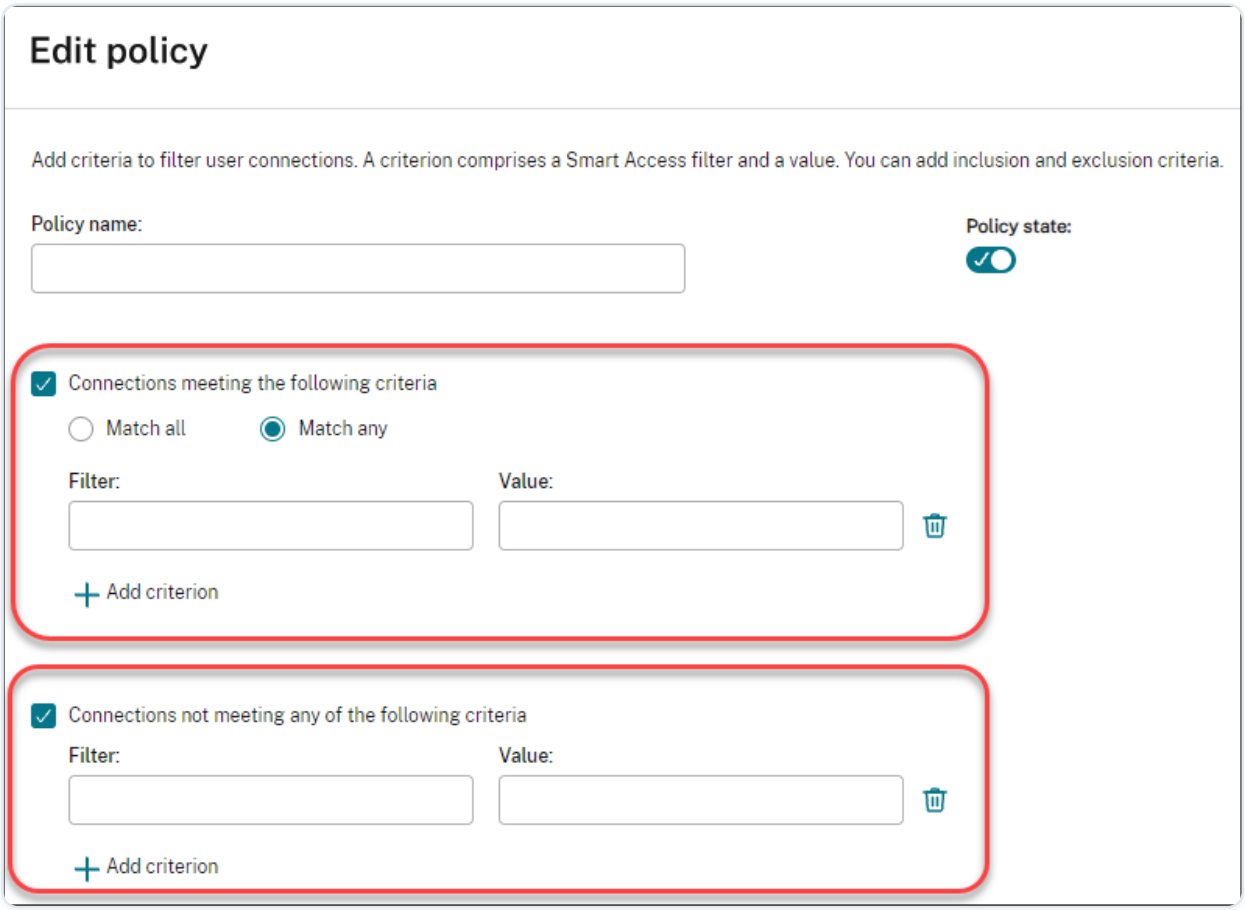
Add access policy rules using Studio

An access policy rule comprises a set of filters. For more information about filters, see this article. When adding an access policy rule, you add multiple condition filters to the rule as needed.

To add a policy for a delivery group using Studio, follow these steps:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **Access Policy** page, click **Add**. The **Add Policy** page appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. In the **Policy name** field, type a descriptive name for the policy. The name must be unique in your deployment.
5. To define the criteria for allowed user connections, follow these steps:
    a. Select **Connections meeting the following criteria**.
    b. Click **Add criterion**.
    c. In the **Filter** field, type the name of the filter that you want to use. In the **Value** field, type a desired value for the filter. For example, to allow only users connected through Workspace (instead of StoreFront) to access resources in this delivery group, type `Citrix-Via-Workspace` for **Filter** and `True` for **Value**.
    d. To add more criteria, repeat steps b-c.
    e. Select the relationship among the criteria:
        - **Match any**. Allows access only when the incoming user connection meets any of the configured filter criteria.
        - **Match all**. Allows access only when the incoming user connection meets all of the configured filter criteria.
6. To define the criteria for prohibited user connections, follow these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Select **Connections not meeting any of the following criteria**.

b. Click **Add criterion**.

c. In the **Filter** field, type the name of the filter that you want to use. In the **Value** field, type a desired value for the filter. For example, to prohibit users connected through the `example.cloud.com` store URL from accessing resources in this delivery group. Type `Citrix.Workspace.UsingDomain` for **Filter** and `example.cloud.com` for **Value**.

d. To add more criteria, repeat steps b-c.

> **NOTE:**
>
> User connections meeting any of the configured criteria are prohibited from resources in this delivery group.

7. Click **Done**.

   The new policy appears in the policy list.

8. Review and refine the default policy rules to avoid unintentional overlaps with connections covered by this new policy. To refine the existing policies, use the following ways:

   - Disable the default policy rules.
   - Configure the default policy rules to exclude the SmartAccess filters that you added to the inclusion criteria of the new policy. For more information, see Manage policy rules using Studio and Add and manage access policy rules using PowerShell.

> **IMPORTANT:**
>
> As explained in About access policy rules, when a user's connection matches one or more policy rules in a delivery group, the user gains access to its resources. Therefore, after creating a rule, you must carefully review and refine the existing rules to avoid any unintentional overlaps with connections covered by the new rule.

Manage access policy rules using Studio

You can use the inclusion and exclusion criteria to refine the default policies. For example, to restrict access to a subset of those connections, follow these steps:

1. Edit a default policy.
2. Select **Connections meeting any of the following criteria**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Add, edit, or remove the SmartAccess policy expressions for the allowed user access scenarios.

For more information, see the Citrix Gateway documentation.

Add and manage access policy rules using PowerShell

You can use the following PowerShell cmdlets to add and manage access policy rules for delivery groups:

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

For more information, see the relative articles in the Citrix Developer Documentation.

Restrict user access to resources across all delivery groups

You can configure resource filtering rules to control user access to applications and desktops across all delivery groups. These rules let you specify the resource type, apply tag-based restrictions, and enforce access conditions based on factors such as network location and store connection context.

Required permission

To perform this task, you must be an administrator role with the **Manage resource filter** permission.

Add a resource filtering rule

To add a resource filtering rule, complete the following steps:

1. Go to **Delivery Groups > Settings**.
2. Select **Manage** in the **Resource filter** tile.
3. In the **Manage resource filter rules** dialog box, click **Add**.
4. Enter a **Name** and **Description** for the rule.
5. Select the resource type that the rule applies to:
    - **Applications**
    - **Desktops**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Both**

6. Select the tag that identifies the resources that the rule applies to.

> **NOTE:**
>
> If you select **Both** as the resource type, selecting a tag is required.

7. Configure the **Smart Access filter** to define the conditions under which the resources are filtered.
8. Click **Add** to save the rule.

Configure user scope for an access policy

By default, all access policies in a delivery group apply to the same set of users. You can configure an access policy to apply to specific users using Studio, PowerShell, or the Rest API.

To apply an access policy to specified users using Studio, follow these steps:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit Delivery Group** in the action bar.
3. On the **Users** page, select **Use contextual access.**
4. Select the access policy that you want to configure, and click **User access scope**. The **User access scope** page appears.
5. To define which authenticated users this policy applies to:
   - To apply this policy to *any* authenticated users, select **Allow any authenticated users to use resources**.
   - To apply this policy to specific users, keep **Restrict use of resources** selected. Then, use the allow list and block list to add or remove users for this policy.
6. To apply this access policy to users who don't provide credentials, select **Grant access to unauthenticated (anonymous) users; no credentials are required**.

Machines

- Manage user assignments for machines
- Enable Local Host Cache for single-session pooled VDAs
- Update a machine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Add, change, or remove a tag restriction for a desktop
- Remove a machine
- Prevent users from connecting to a machine (maintenance mode)
- Shut down and restart machines
- Create and manage restart schedules for machines
- Enable a one-time restart schedule
- Manage Autoscale™

In addition to the features described in this article, see Autoscale for information about proactively power managing machines.

Manage user assignments for machines

NOTE:

This task is available only for MCS-provisioned single-session static machines.

Manage user assignments for machines in a delivery group. When desktop assignment rules are configured for the delivery group, machines are randomly assigned to users upon initial desktop launch and remain assigned to the users unless their user assignments are modified. If you want to manually assign an unassigned machine to specific users or change the existing user assignment for a machine, follow the steps described in this task to make changes. Using these steps, you can also modify names displayed in the Citrix Workspace App for machines assigned to users.

Detailed steps are as follows:

1. From Studio, select **Delivery Groups** from the left pane.
2. Select a group, and then select **Edit** in the action bar.
3. In the left pane, select **Machine Allocation**. The following details for each machine in the group appear:
    - **Machine name:** Shows the name of a machine.
    - **Display name:** Shows the machine's display name in Citrix Workspace App.
    - **Users:** Shows users assigned to this machine. If desktop assignment rules are configured, machines are randomly assigned to users upon their initial desktop launch and remain assigned to them unless their user assignments are modified.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Locate a machine, and then assign users to it or change its user assignment:
    - Click **Browser** to browser to users.
    - In the **Users** column, enter a semicolon-separated list of user names.
    - Click **Import from CSV file** to import the setting details using a CSV file.
    - Click **Change** to update the machine's desktop icon from an `.ico` or an `.exe` file. The specified icon overrides the default icon set only at the machine level.
5. (Optional) If the machine is assigned to users, modify its display name as needed.

    NOTE:

    The Display name field is enabled only when the machine is assigned to users:

    - If the machine is assigned to a user based on a desktop assignment rule, this field shows the display name configured in that rule.
    - If the machine is manually assigned to users and the field is left blank, the delivery group's published name (if specified) is used as the machine's display name. The delivery group's name is used if the published name is unspecified. You can specify published names for delivery groups only through PowerShell.
6. Select **Apply** to apply changes and keep the window open. Or, select **OK** to apply changes and close the window.

Enable Local Host Cache for single-session pooled VDAs

By default, power-managed, single-session, pooled machines can be used for only one session when in Local Host Cache mode. You can override the default behavior on a per-delivery group basis. Detailed steps are as follows:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group as needed, then select **Edit** in the action bar.
3. On the **Local Host Cache** page, select **Use machines for subsequent sessions**.
4. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

Alternatively, you can override the default behavior using PowerShell commands. For more information, see Enable using PowerShell.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

Enabling access to power-managed single-session pooled machines can cause data and changes from previous user sessions being present in subsequent sessions.

Update a machine in a delivery group

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **View Machines** in the action bar.
3. Select a machine and then select **Update Machines** in the action bar.

To choose a different image, select **Image** and then select a snapshot.

To apply changes and notify machine users, select **Rollout notification to end-users**. Then specify:

- When to update the image: now or on the next restart
- The restart distribution time (the total time to begin updating all machines in the group)
- Whether users are notified of the restart
- The message users will receive

Add, change, or remove a tag restriction for a desktop

Adding, changing, and removing tag restrictions can have unanticipated effects on which desktops are considered for launch. Review the considerations and cautions in Tags.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the Actions bar.
3. On the **Desktops** page, select the desktop and select **Edit**.
4. To add a tag restriction, select **Restrict launches to machines with the tag** and then select the tag.
5. To change or remove a tag restriction, either:
    - Select a different tag.
    - Remove the tag restriction by clearing **Restrict launches to machines with this tag**.
6. Select **Apply** to apply any changes you made and keep the window open. Or, select **OK** to apply changes and close the window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remove a machine from a delivery group

Removing a machine deletes it from a delivery group. It does not delete it from the machine catalog that the delivery group uses. Therefore, that machine is available for assignment to another delivery group.

Machines must be shut down before they can be removed. To temporarily stop users from connecting to a machine while you are removing it, put the machine into maintenance mode before shutting it down.

Machines might contain personal data, so use caution before allocating the machine to another user. Consider reimaging the machine.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **View Machines** in the action bar.
3. Ensure that the machine is shut down.
4. Select the machine and then select **Remove from Delivery Group** in the action bar.

You can also remove a machine from a delivery group through the connection the machine uses.

Prevent users from connecting to a machine (maintenance mode) in a delivery group

When you need to temporarily stop new connections to machines, you can turn on maintenance mode for one or all machines in a delivery group. You might do this before applying patches or using management tools.

- When a multi-session OS machine is in maintenance mode, users can connect to existing sessions, but cannot start new sessions.
- When a single-session OS machine (or a PC using Remote PC Access) is in maintenance mode, users cannot connect or reconnect. Current connections remain connected until they disconnect or log off.

To turn maintenance mode on or off:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group.
3. To turn on maintenance mode for all machines in the delivery group, select **Turn On Maintenance Mode** in the action bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To turn on maintenance mode for one machine, select **View Machines** in the action bar. Select a machine, and then select **Turn On Maintenance Mode** in the action bar.

4. To turn maintenance mode off for one or all machines in a delivery group, follow the previous instructions, but select **Turn Off Maintenance Mode** in the action bar.

Windows Remote Desktop Connection (RDC) settings also affect whether a multi-session OS machine is in maintenance mode. Maintenance mode is on when any of the following occur:

- Maintenance mode is set to on, as described earlier.
- RDC is set to **Don't allow connections to this computer**.
- RDC is not set to **Don't allow connections to this computer** and the Remote Host Configuration User Logon Mode setting is either **Allow reconnections, but prevent new logons** or **Allow reconnections, but prevent new logons until the server is restarted**.

You can also turn maintenance mode on or off for:

- A connection, which affects the machines using that connection.
- A machine catalog, which affects the machines in that catalog.

Shut down and restart machines in a delivery group

This procedure is not supported for Remote PC Access machines.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **View Machines** in the action bar.
3. Select the machine and then select one of the following actions in the action bar:

NOTE:

- The following actions apply only to machines that are power managed.
- Some options might not be available, depending on the machine state.

- **Force shut down:** Forcibly powers off the machine and refreshes the list of machines.
- **Restart:** Requests the operating system to shut down and then start the machine again. If the operating system cannot comply, the machine remains in its current state.
- **Force restart:** Forcibly shuts down the operating system and then restarts the machine.
- **Suspend:** Pauses the machine without shutting it down, and refreshes the list of machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Shut down:** Requests the operating system to shut down.

For non-force actions, if the machine does not shut down within 10 minutes, it is powered off. If Windows attempts to install updates during the shutdown, there is a risk that the machine will be powered off before the updates finish.

Create and manage restart schedules for machines in a delivery group

NOTE:

- When a restart schedule is applied to a delivery group with Autoscale enabled, its machines are just powered off and left for Autoscale to power them on.
- When restart schedules are applied to random single-session machines, those machines are powered off rather than restarted, to save costs. We recommend that you use Autoscale to power on machines.
- Changing the time zone on a delivery group might reboot the machines in that delivery group. To avoid this, ensure to change the time zone settings outside of production hours.

A restart schedule specifies when machines in a delivery group are periodically restarted. You can create one or more schedules for a delivery group. A schedule can affect either:

- All the machines in the group.
- One or more (but not all) machines in the group. The machines are identified by a tag that you apply to the machine. This is called a tag restriction, because the tag restricts an action to only items (in this case, machines) that have the tag.

For example, let's say all of your machines are in one delivery group. You want every machine restarted once every week, and you want the machines used by the accounting team restarted daily. To accomplish this, set up one schedule for all machines, and another schedule for only the machines in accounting.

A schedule includes the day and time that the restart begins, and the duration. The duration is either "start all affected machines at the same time" or an interval it will likely take to restart all affected machines.

You can enable or disable a schedule. Disabling a schedule can be helpful when testing, during special intervals, or when preparing schedules before you need them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You cannot use schedules for automated power-on or shutdown from the management console, only to restart.

Schedule overlap

Multiple schedules can overlap. In the example above, both schedules affect the accounting machines. Those machines might be restarted twice on Sunday. The scheduling code is designed to avoid restarting the same machine more often than intended, but it cannot be guaranteed.

- If the schedules coincide precisely in start and duration times, it is more likely that the machines will be restarted only once.
- The more the schedules differ in start and duration times, it's more likely that multiple restarts will occur.
- The number of machines affected by a schedule also affects the chance of an overlap. In the example, the weekly schedule that affects all machines might initiate restarts faster than the daily schedule for accounting machines, depending on the duration specified for each.

For an in-depth look at restart schedules, see Reboot schedule internals.

View restart schedules

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. Select the **Restart Schedule** page.

The **Restart Schedule** page contains the following information for each configured schedule:

- Schedule name.
- Tag restriction used, if any.
- How often the machine restarts occur.
- Whether machine users receive a notification.
- Whether the schedule is enabled. Disabling a schedule can be helpful when testing, during special intervals, or when preparing schedules before you need them.

Add (apply) tags

When you configure a restart schedule that uses a tag restriction, ensure that the tag has been added (applied) to the machines that the schedule affects. In the example above, each of the machines used by the accounting team has a tag applied. For details, see Tags.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Although you can apply more than one tag to a machine, a restart schedule can specify only one tag.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select the group containing the machines to be controlled by the schedule.
3. Select **View Machines** and then select the machines you want to add a tag to.
4. Select **Manage Tags** in the action bar.
5. If the tag exists, enable the check box next to the tag name. If the tag does not exist, select **Create** and then specify the name for the tag. After the tag is created, enable the check box next to the newly created tag name.
6. Select **Save** in the **Manage Tags** dialog.

Create a restart schedule

NOTE:

Restart schedules can be applied to all power managed and non-power managed multi-session machines.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Restart Schedule** page, select **Add**.
4. On the **Add Restart Schedule** page:
   - To enable the schedule, select **Yes**. To disable the schedule, select **No**.
   - Type a schedule name and description.
   - For **Restrict to tag**, apply a tag restriction.
   - For **Include machines in maintenance mode**, choose whether to include machines that are in maintenance mode in this schedule. To use PowerShell instead, see Scheduled restarts for machines in maintenance mode.
   - For **Restart frequency**, select how often the restart occurs: daily, weekly, monthly, or once. If you select **Weekly** or **Monthly**, you can specify one or more specific days.
   - For **Repeats every**, specify how often you want the schedule to run.
   - For **Start date**, specify a start date for the first occurrence of the schedule.
   - For **Begin restart at**, specify, in 24-hour clock format, the time of day to begin the restart.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For **Restart duration**:
  - To forcibly restart machines with unresponsive sessions, select **Forced restart**, then select one of the following options:
    - **Restart all machines at once**
    - **Restart all machines within a time period**, and specify the time by **Hour** or **Minute**.
  - To wait for all sessions to drain before restarting, select **Graceful restart**.

    Upon starting a restart schedule that is configured to use graceful restart:
    - All idle machines belonging to the delivery group are restarted immediately
    - Each machine belonging to the delivery with one or more active sessions are restarted when all sessions are logged off.

    NOTE:

    Graceful restart schedules can only restart power managed machines.
- In **Send notification to users**, determine whether to display a notification message on the applicable machines before a restart begins. By default, no message appears.
- If you choose to display a message 15 minutes before the restart begins, you can choose to repeat the message every five minutes after the initial message. By default, the message does not repeat.
- Enter the notification title and text. There is no default text.

  If you want the message to include a countdown to restart, include the variable **%m%**. Unless you chose to restart all machines at the same time, the message appears on each machine at the appropriate time before the restart.

5. Click **Done** to apply the changes and to close the **Add Restart Schedule** window.
6. Click **Apply** to apply the changes you made and keep the **Edit Delivery Group** window open. Or, click **Save** to apply changes and to close the window.

Immediately run a restart schedule

A restart schedule specifies when machines in a delivery group restart regularly. You can also run a restart schedule immediately to restart the machines in that schedule.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To run a restart schedule immediately, follow these steps:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select the applicable delivery group and then select **Edit** in the action bar
3. On the **Restart Schedule** page, select a schedule that you want to run and then select **Run schedule now**.

NOTE:

- You cannot run a schedule immediately if it is configured with the **Restart all machines after draining sessions** setting.
- You can apply **Run schedule now** only to one schedule at a time.
- After you edit a schedule, **Run schedule now** becomes unavailable. Select **Apply** to make it available.

Edit, remove, enable, or disable a restart schedule

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Restart Schedule** page, select the check box for a schedule.
    - To edit a schedule, select **Edit**. Update the schedule configuration, using the guidance in Create a restart schedule.
    - To enable or disable a schedule, select **Edit**. Select or clear the **Enable restart schedule** check box.
    - To remove a schedule, select **Remove**. Confirm the removal. Removing a schedule does not affect any tags applied to machines in the affected machines.

Scheduled restarts delayed due to database outage

NOTE:

This feature is available only in PowerShell.

If a site database outage occurs before a scheduled restart begins for machines (VDAs) in a delivery group, the restarts begin when the outage ends. This action can have unintended results.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, let's say you've scheduled a delivery group's restarts to occur during off-production hours (beginning at 3 am). A site database outage occurs one hour before a scheduled restart begins (2 am). The outage lasts six hours (until 8 am). The restart schedule begins when the connection between the Delivery Controller™ and the site database is restored. The VDA restarts now begin five hours after their original schedule. This action might result in VDAs restarting during production hours.

To help avoid this situation, you can use the `MaxOvertimeStartMins` parameter for the `New-BrokerRebootScheduleV2` and `Set-BrokerRebootScheduleV2` cmdlets. The value specifies the maximum number of minutes beyond the scheduled start time that a restart schedule can begin.

- If the database connection is restored within that time (scheduled time + `MaxOvertimeStartMins`), the VDA restarts begin.
- If the database connection is not restored within that time, the VDA restarts do not begin.
- If this parameter is omitted or has a zero value, the scheduled restart begins when the connection to the database is restored, regardless of the outage duration.

For more information, see the cmdlet help. This feature is available only in PowerShell.

Scheduled restarts for machines in maintenance mode

To indicate whether a restart schedule affects machines that are in maintenance mode, use the `IgnoreMaintenanceMode` option with the `BrokerRebootScheduleV2` cmdlets.

For example, the following cmdlet creates a schedule that restarts both machines that are and machines that are not in maintenance mode.

```
New-BrokerRebootSchedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

The following cmdlet modifies an existing restart schedule.

```
Set-BrokerRebootSchedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

For more information, see the cmdlet help.

Enable a one-time restart schedule

If you want to enable one-time restart schedule using PowerShell, use the following `BrokerCatalogRebootSchedule` PowerShell commands to create, modify, and delete a restart schedule:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Get-BrokerCatalogRebootSchedule`
- `New-BrokerCatalogRebootSchedule`
- `Set-BrokerCatalogRebootSchedule`
- `Remove-BrokerCatalogRebootSchedule`
- `Rename-BrokerCatalogRebootSchedule`

Limitations:

- A catalog reboot schedule associated with a catalog that is without a configured timezone is created but does not start.
- When a catalog reboot schedule is created, then the reboot schedule runs only on the catalog VMs belonging to a delivery group.

Example:

- To create a restart schedule of the VMs in the catalog named **BankTellers** to begin on Feb 3, 2022, between 2 AM and 4 AM.

```
New-BrokerCatalogRebootSchedule -Name BankTellers

-CatalogName BankTellers

-StartDate "2022-02-03"

-StartTime "02:00"

-Enabled $true

-RebootDuration 120
```

- To create a restart schedule of the VMs in the catalog having UID 17 to begin on Feb 3, 2022, between 1 AM and 5 AM. Ten minutes before the restart, each VM is set to display a message box with the title: **WARNING: Reboot pending**, and the message: **Save your work**, in every user session.

```
New-BrokerCatalogRebootSchedule

-Name 'Update reboot'

-CatalogUid 17
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-StartDate "2022-02-03"

-StartTime "01:00" -Enabled $true -RebootDuration 240

-WarningTitle "WARNING: Reboot pending"

-WarningMessage "Save your work" -WarningDuration 10
```

- To rename the catalog restart the schedule named **Old Name** to **New Name**.

```
Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName "New Name"
```

- To display all catalog restart schedules with UID 1, and then rename the catalog reboot schedule with the UID 1 to **New Name**.

```
Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- To set the catalog restart schedule named **Accounting** to display a message with the title **WARNING: Reboot pending, and the message, Save your work**, ten minutes before the restart of each VM. The message appears in every user session on that VM.

```
Set-BrokerCatalogRebootSchedule -Name Accounting

-WarningMessage "Save your work"

-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
```

- To display all restart schedules that are disabled, and then enable all disabled restart schedules.

```
Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- To set the catalog restart schedule with UID 17 to display the message: **Rebooting in %m% minutes** in fifteen, ten, and five minutes before the restart of each VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in %m%
minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- To configure the time zone for the catalog named **MyCatalog**.

```
Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
```

Manage Autoscale

By default, Autoscale is disabled for delivery groups. To manage Autoscale for a delivery group (if applicable), follow these steps:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Manage Autoscale** in the action bar. The **Manage Autoscale** window appears.
3. Configure settings as needed. For information about Autoscale settings, see Autoscale.
4. Select **Apply** to apply any changes you made and to keep the window open. Or, select **Save** to apply changes and to close the window.

Sessions

- Log off or disconnect a session, or send a message to users
- Configure session prelaunch and session linger
- Configure session roaming
- Control session reconnection when disconnected from machine in maintenance mode

Log off or disconnect a session, or send a message to delivery group users

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **View Machines** in the action bar.
3. To log a user off a session, select the session or desktop and then select **Log off** in the action bar. The session closes and the machine becomes available to other users, unless it is allocated to a specific user.
4. To disconnect a session, select the session or desktop and then select **Disconnect** in the action bar. Applications continue to run and the machine remains allocated to that user. The user can reconnect to the same machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. To send a message to users, select the session, machine, or user and then select **Send message** in the action bar. Enter the message.

Configure session prelaunch and session linger in a delivery group

These features are supported only on multi-session OS machines.

The session prelaunch and session linger features help specified users access applications quickly, by:

- Starting sessions before they are requested (session prelaunch)
- Keeping application sessions active after a user closes all applications (session linger)

By default, session prelaunch and session linger are not used. A session starts (launches) when a user starts an application, and remains active until the last open application in the session closes.

Considerations:

- The delivery group must support applications, and the machines must be running a VDA for multi-session OS, minimum version 7.6.
- These features are supported only when using Citrix Workspace app for Windows, and also require more Citrix Workspace app configuration. For instructions, search for session prelaunch in the product documentation for your Citrix Workspace app for Windows version.
- Citrix Workspace app for HTML5 is not supported.
- When using session prelaunch, if a user's machine is put into suspend or hibernate mode, prelaunch does not work (regardless of session prelaunch settings). Users can lock their machines/sessions. However, if a user logs off from Citrix Workspace app, the session is ended and prelaunch no longer applies.
- When using session prelaunch, physical client machines cannot use the suspend or hibernate power management functions. Client machine users can lock their sessions but should not log off.
- If using a user/device license, the license lasts 90 days. Unused prelaunched and lingering sessions disconnect after 15 minutes by default. You can configure the timeout value in PowerShell (`New/Set-BrokerSessionPreLaunch` cmdlet).
- Careful planning and monitoring of your users' activity patterns are essential to tailoring these features to complement each other. Optimal configuration balances the benefits of earlier application availability for users against the cost of keeping licenses in use and resources allocated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can also configure session prelaunch for a scheduled time of day in Citrix Workspace app.

How long unused prelaunched and lingering sessions remain active

There are several ways to specify how long an unused session remains active if the user does not start an application: a configured timeout and server load thresholds. You can configure all of them. The event that occurs first causes the unused session to end.

- **Timeout:** A configured timeout specifies the number of minutes, hours, or days an unused prelaunched or lingering session remains active. If you configure too short a timeout, prelaunched sessions end before they provide the user benefit of quicker application access. If you configure too long a timeout, incoming user connections might be denied because the server doesn't have enough resources.

  You can enable this timeout from the SDK only (`New/Set-BrokerSessionPreLaunch` cmdlet), not from the management console. If you disable the timeout, it does not appear in the console display for that delivery group or in the **Edit Delivery Group** pages.
- **Thresholds:** Automatically ending prelaunched and lingering sessions based on server load ensures that sessions remain open as long as possible, assuming that server resources are available. Unused prelaunched and lingering sessions do not cause denied connections because they are ended automatically when resources are needed for new user sessions.

  You can configure two thresholds: the average percentage load of all servers in the delivery group, and the maximum percentage load of a single server in the group. When a threshold is exceeded, the sessions that have been in the prelaunch or lingering state for the longest time are ended. Sessions are ended one-by-one at minute intervals until the load falls below the threshold. While the threshold is exceeded, no new prelaunch sessions are started.

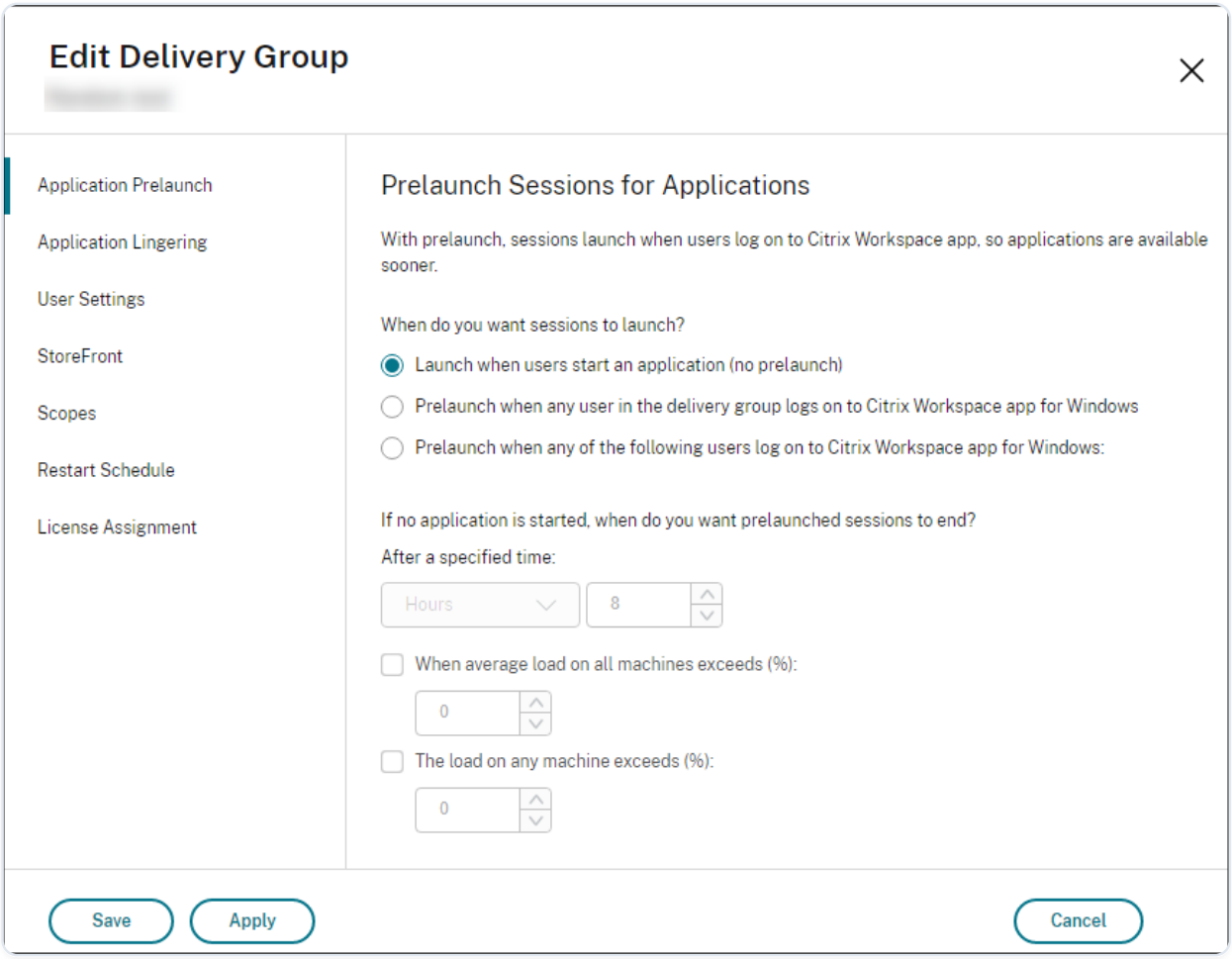
Servers with VDAs that have not registered with a Controller and servers in maintenance mode are considered fully loaded. An unplanned outage causes prelaunch and lingering sessions to end automatically to free capacity.

To enable session prelaunch

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Application Prelaunch** page, enable session prelaunch by choosing when sessions launch:
   - When a user starts an application. This is the default setting. Session prelaunch is disabled.
   - When any user in the delivery group logs on to Citrix Workspace app for Windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When anyone in a list of users and user groups logs on to Citrix Workspace app for Windows. Be sure to also specify users or user groups if you choose this option.



4. A prelaunched session is replaced with a regular session when the user starts an application. If the user does not start an application (the prelaunched session is unused), the following settings affect how long that session remains active.

   - When a specified time interval elapses. You can change the time interval (1–99 days, 1–2376 hours, or 1–142,560 minutes).
   - When the average load on all machines in the delivery group exceeds a specified percentage (1–99%).
   - When the load on any machine in the delivery group exceeds a specified percentage (1–99%).

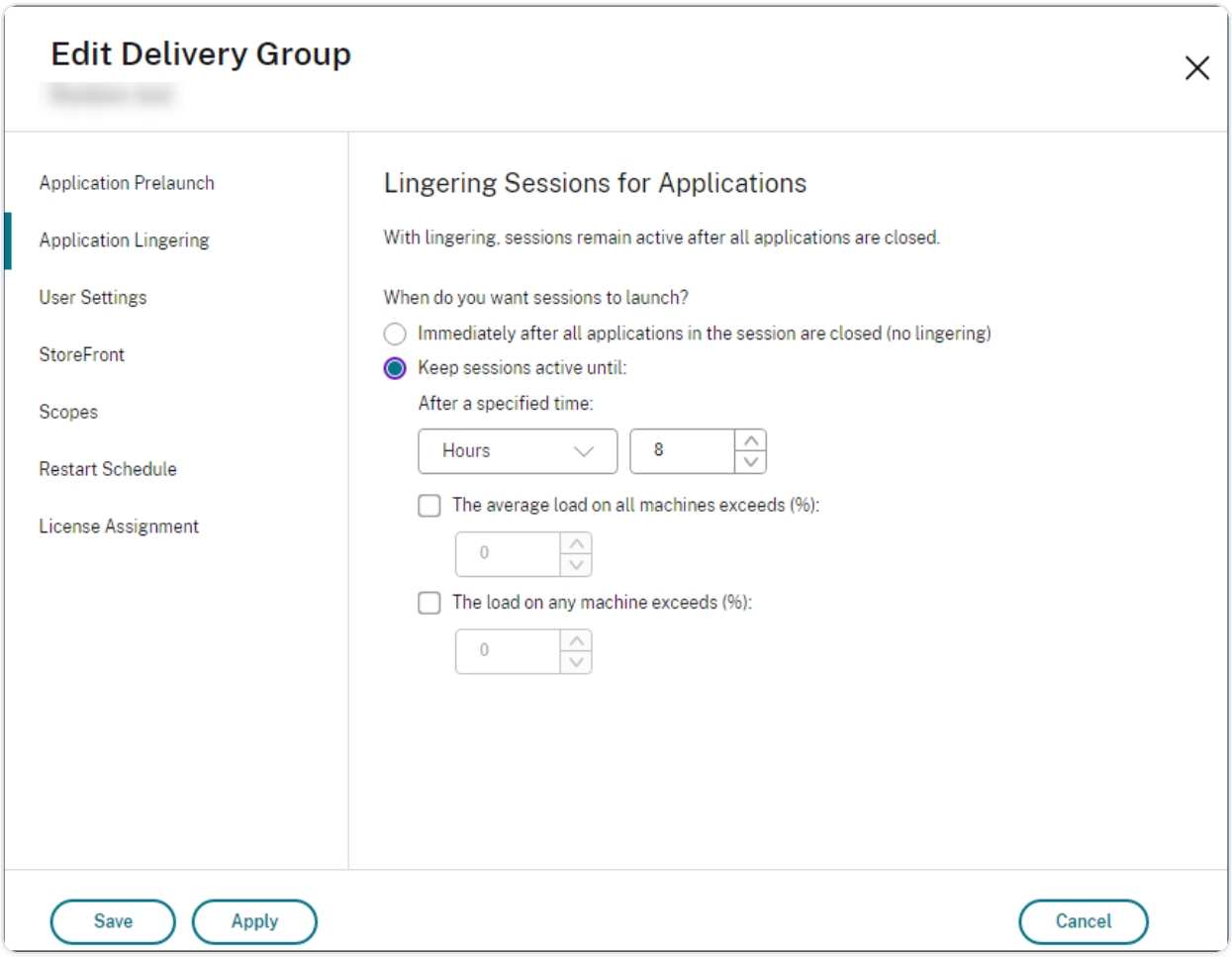
   Recap: A prelaunched session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

To enable session linger

1. From Studio, select **Delivery Groups** in the left pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select a group and then select **Edit** in the action bar.
3. On the **Application Lingering** page, enable session linger by selecting **Keep sessions active until**.



4. Several settings affect how long a lingering session remains active if the user does not start another application.

   - When a specified time interval elapses. You can change the time interval: 1–99 days, 1–2376 hours, or 1–142,560 minutes.
   - When the average load on all machines in the delivery group exceeds a specified percentage: 1–99%.
   - When the load on any machine in the delivery group exceeds a specified percentage: 1–99%.

   Recap: A lingering session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure session roaming

By default, session roaming is enabled for delivery groups. Sessions roam between client devices with the user. When the user launches a session and then moves to another device, the same session is used and applications are simultaneously available on both devices. You can view the applications on multiple devices. The applications follow, regardless of the device or whether current sessions exist. Often, printers and other resources assigned to the application also follow. Alternatively, you can also use PowerShell. For more information, see Session roaming.

Configure session roaming for applications

To configure session roaming for applications, follow these steps:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit Delivery Group** in the action bar.
3. On the **Users** page, enable session roaming by selecting the **Sessions roam with users as they move between devices** check box.
    - When enabled, if a user launches an application session and then moves to another device, the same session is used and available on both devices. When disabled, the session no longer roams between devices.
4. Select **OK** to apply changes and close the window.

Configure session roaming for desktops

To configure session roaming for a desktop, follow these steps:

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit Delivery Group** in the action bar.
3. On the **Desktops** page, select the desktop and select **Edit**.
4. Enable session roaming by selecting the **Session roaming** check box.
    - When enabled, if the user launches the desktop and then moves to another device, the same session is used, and applications are available on both devices. When disabled, the session no longer roams between devices.
5. Select **OK** to apply changes and close the window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Control session reconnection when disconnected from machine in maintenance mode

NOTE:

This feature is available only in PowerShell.

You can control whether sessions that are disconnected on machines in maintenance mode are allowed to reconnect to machines in the delivery group.

Before late May 2021, reconnection was not allowed for single-session pooled desktop sessions that had disconnected from machines in maintenance mode. Now, you can configure a delivery group to allow or prohibit reconnections (regardless of session type) after disconnection from a machine in maintenance mode.

When creating or editing a delivery group (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), use the `-AllowReconnectInMaintenanceMode <boolean>` parameter to allow or prohibit reconnections for machines that were disconnected from a machine in maintenance mode.

- When set to true, sessions can reconnect to machines in the group.
- When set to false, sessions cannot reconnect to machines in the group.

Default values:

- Single-session: Disabled
- Multi-session: Enabled

Applications

View applications in a delivery group and add more if needed.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select a group. If this group contains applications, **View Applications** appears in the action bar.
3. Select **View Applications**. You are directed to the **Applications** node where all applications available in this group appear.
4. To add more applications to this group, go to the **Delivery Groups** node, select the group, and select **Add Applications** in the action bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot

- VDAs that are not registered with a Delivery Controller are not considered when launching brokered sessions. This results in underutilization of otherwise available resources. There are various reasons a VDA might not be registered, many of which an administrator can troubleshoot. The details display provides troubleshooting information in the catalog creation wizard, and after you add a catalog to a delivery group.

  After you create a delivery group, the details pane for a delivery group indicates the number of machines that are expected to be registered but are not. For example, one or more machines are powered on and not in maintenance mode, but are not currently registered with a Controller. When viewing a "not registered, but should be" machine, review the **Troubleshoot** tab in the details pane for possible causes and recommended corrective actions.

  For messages about functional level, see VDA versions and functional levels.

  For information about VDA registration troubleshooting, seeCTX136668.

- In the display for a delivery group, the **Installed VDA version** in the details pane might differ from the actual version installed on the machines. The machine's Windows Programs and Features display shows the actual VDA version.
- For machines with **Power State Unknown** status, see CTX131267 for guidance.

Create application groups

Introduction

Application groups let you manage collections of applications. You can create application groups for applications shared across different delivery groups or used by a subset of users within delivery groups. Application groups are optional. They offer an alternative to adding the same applications to multiple delivery groups. Delivery groups can be associated with more than one application group, and an application group can be associated with more than one delivery group.

Using application groups can provide application management and resource control advantages over using more delivery groups:

- The logical grouping of applications and their settings lets you manage those applications as a single unit. For example, you don't have to add (publish) the same application to individual delivery groups one at a time.
- Session sharing between application groups can conserve resource consumption. In other cases, disabling session sharing between application groups may be beneficial.

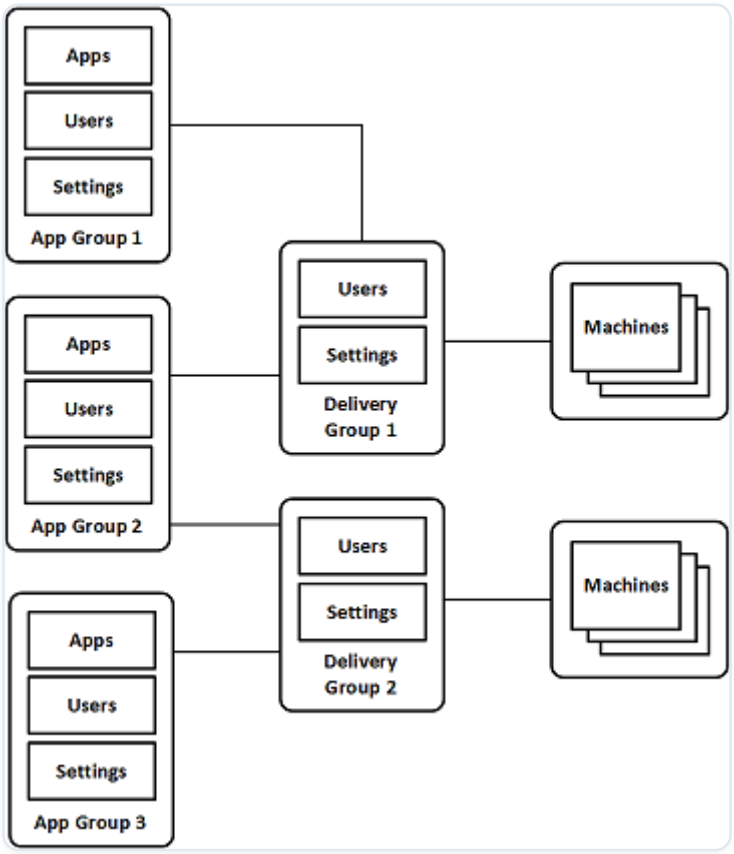
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can use the tag restriction feature to publish applications from an application group, considering only a subset of the machines in selected delivery groups. With tag restrictions, you can use your existing machines for more than one publishing task, saving the costs associated with deploying and managing additional machines. A tag restriction can be thought of as subdividing (or partitioning) the machines in a delivery group. Using an application group or desktops with a tag restriction can be helpful when isolating and troubleshooting a subset of machines in a delivery group.

Example configurations

Example 1

The following graphic shows a deployment that includes application groups:



In this configuration, applications are added to the application groups, not the delivery groups. The delivery groups specify which machines will be used. (Although not shown, the machines are in machine catalogs.)

Application group 1 is associated with delivery group 1. The applications in application group 1 can be accessed by the users specified in application group 1, as long as they are also in the user list for delivery group 1. This follows the guidance that the user list for an application group should be a subset (a restriction) of the user lists for the associated delivery groups. The settings in application group 1 (such as application session sharing between application groups, associated delivery

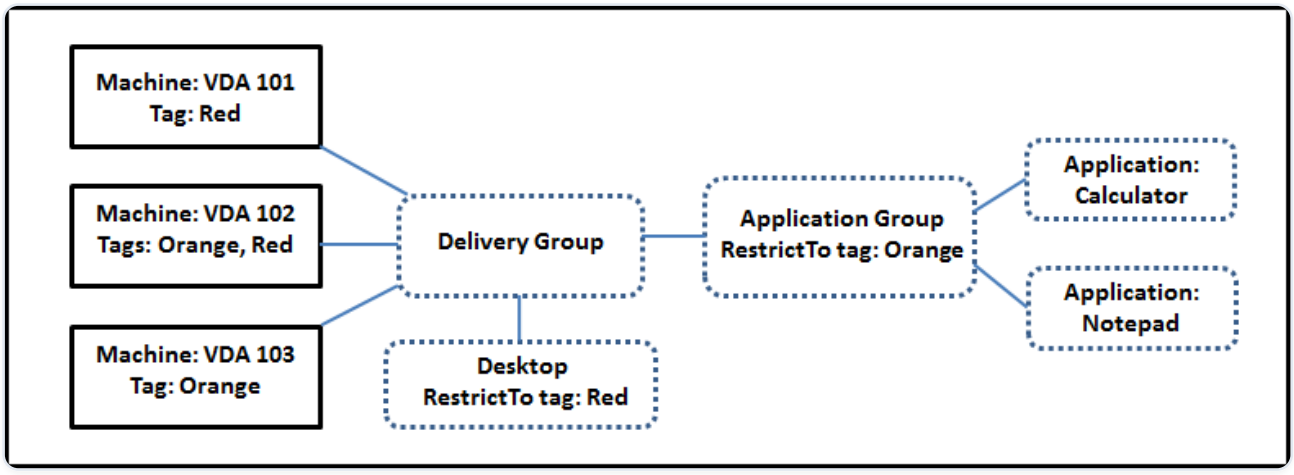
© 1997–2026 Citrix Systems, Inc. All rights reserved.

groups) apply to applications and users in that group. The settings in delivery group 1 (such as anonymous user support) apply to users in application groups 1 and 2, because those application groups have been associated with that delivery group.

Application group 2 is associated with two delivery groups: 1 and 2. Each of those delivery groups can be assigned a priority in application group 2, which indicates the order in which the delivery groups will be checked when an application is launched. delivery groups with equal priority are load balanced. The applications in application group 2 can be accessed by the users specified in application group 2, as long as they are also in the user lists for delivery group 1 and delivery group 2.

Example 2

This simple layout uses tag restrictions to limit which machines will be considered for certain desktop and application launches. The site has one shared delivery group, one published desktop, and one application group configured with two applications.



Tags have been added to each of the three machines (VDA 101-103).

The application group was created with the "Orange" tag restriction, so each of its applications (Calculator and Notepad) can be launched only on machines in that delivery group that have the tag "Orange": VDA 102 and 103.

For more comprehensive examples and guidance for using tag restrictions in application groups (and for desktops), see Tags.

Guidance and considerations

Citrix® recommends adding applications to either application groups or delivery groups, but not both. Otherwise, the additional complexity of having applications in two group types can make it more difficult to manage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, an application group is enabled. After you create an application group, you can edit the group to change this setting. See Manage application groups.

By default, application session sharing between application groups is enabled. See Session sharing between application groups.

Citrix recommends upgrading your delivery groups to the current version. This requires:

1. Upgrading VDAs on the machines used in the delivery group.
2. Changing to a higher function level for the machine catalogs containing those machines
3. Changing to a higher function level for the delivery group.

For details, see Manage delivery groups.

To use application groups, your core components must be minimum version 7.9.

Creating application groups requires the delegated administration permission of the Delivery Group Administrator built-in role. See Delegated administration for details.

This article refers to "associating" an application with more than one application group to differentiate that action from adding a new instance of that application from an available source. Similarly, delivery groups are associated with application groups (and vice versa), rather than being additions or components of one another.

Session sharing with application groups

When application session sharing is enabled, all applications launch in the same application session. This saves the costs associated with launching additional application sessions, and allows the use of application features that involve the clipboard, such as copy-paste operations. However, in some situations you may wish to turn off session sharing.

When you use application groups you can configure application session sharing in the following three ways which extend the standard session sharing behavior available when you are using only delivery groups:

- Session sharing enabled between application groups.
- Session sharing enabled only between applications in the same application group.
- Session sharing disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session sharing between application groups

You can enable application session sharing between application groups, or you can disable it to limit application session sharing only to applications in the same application group.

- **An example when enabling session sharing between application groups is helpful:**

  Application group 1 contains Microsoft Office applications such as Word and Excel. Application group 2 contains other applications such as Notepad and Calculator, and both application groups are attached to the same delivery group. A user who has access to both application groups starts an application session by launching Word, and then launches Notepad. If the user's existing session running Word is suitable for running Notepad then Notepad is started within the existing session. If Notepad cannot be run from the existing session—for example if the tag restriction excludes the machine that the session is running on—then a new session on a suitable machine is created rather than using session sharing.

- **An example when disabling session sharing between application groups is helpful:**

  You have a set of applications that do not interoperate well with other applications that are installed on the same machines, such as two different versions of the same software suite or two different versions of the same web browser. You prefer not to allow a user to launch both versions in the same session.

  You create an application group for each version of the software suite, and add the applications for each version of the software suite to the corresponding application group. If session sharing between groups is disabled for each of those application groups, a user specified in those groups can run applications of the same version in the same session, and can still run other applications at the same time, but not in the same session. If the user launches one of the different-versioned applications (that are in a different application group), or launches any application that is not contained in an application group, then that application is launched in a new session.

This session sharing between application groups feature is not a security sandboxing feature. It is not foolproof, and it cannot prevent users from launching applications into their sessions through other means (for example, through Windows Explorer).

If a machine is at capacity, new sessions are not started on it. New applications are started in existing sessions on the machine as needed using session sharing (providing that this complies with the session sharing restrictions described here).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can only make prelaunched sessions available to application groups which have application session sharing allowed. (Sessions which use the session linger feature are available to all application groups.) These features must be enabled and configured in each of the delivery groups associated with the application group. You cannot configure them in the application groups.

By default, application session sharing between application groups is enabled when you create an application group. You cannot change this when you create the group. After you create an application group, you can edit the group to change this setting. See Manage application groups.

Disable session sharing within an application group

You can prevent application session sharing between applications which are in the same application group.

- **An example when disabling session sharing within application groups is helpful:**

  You want your users to access multiple simultaneous full screen sessions of an application on separate monitors.

  You create an application group and add the applications to it. If session sharing is prohibited between applications in that application group, when a user specified in it starts one application after another they launch in separate sessions, and the user can move each to a separate monitor.

By default, application session sharing is enabled when you create an application group. You cannot change this when you create the group. After you create an application group, you can edit the group to change this setting. See Manage application groups.

Create an application group

Use the process of creating an Application Group to create Application Categories in the Citrix Workspace™ app. Application Categories allow you to manage collections of applications in Citrix Workspace app.

To create an application group:

1. From Studio, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. To organize application groups using folders, create folders under the **Application Groups** root folder. For more information, see Organize application groups using folders.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select the folder where you want to create the group, and then click **Create Application Group**. The group creation wizard launches with an **Introduction** page. You can remove the page from future launches of this wizard.
4. Follow the wizard to configure settings on the pages described below. When you are done with each page, select **Next** until you reach the **Summary** page.

Step 1. Delivery groups

The **Delivery Groups** page lists all delivery groups, with the number of machines each group contains.

- The **Compatible Delivery Groups** list contains delivery groups you can select. Compatible delivery groups contain random (not permanently or statically assigned) server or desktop OS machines.
- The **Incompatible Delivery Groups** list contains delivery groups you cannot select. Each entry explains why it is not compatible, such as containing static assigned machines.

An application group can be associated with delivery groups containing shared (not private) machines that can deliver applications.

You can also select delivery groups containing shared machines that deliver only desktops, if both of the following conditions are met:

- The delivery group contains shared machines and was created with a XenDesktop version earlier than 7.9.
- You have Edit Delivery Group permission.

The delivery group type is automatically converted to "desktops and applications" when the group creation wizard is committed.

Although you can create an application group that has no associated delivery groups (perhaps to organize applications or to serve as storage for applications not currently used) the application group cannot be used to deliver applications until it specifies at least one delivery group. Additionally, you cannot add applications to the application group from the **From Start** menu source if there are no delivery groups specified.

The delivery groups you select specify the machines that will be used to deliver applications. Select the check boxes next to the delivery groups you want to associate with the application group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To add a tag restriction, select **Restrict launches to machines with the tag** and then select the tag from the dropdown.

Step 2. Users

Specify who can use the applications in the application group. You can either allow all users and user groups in the delivery groups you selected on the previous page, or select specific users and user groups from those delivery groups. If you restrict use to users you specify, then only the users specified in the delivery group and the application group can access the applications in this application group. Essentially, the user list in the application group provides a filter on the user lists in the delivery groups.

Enabling or disabling application use by unauthenticated users is available only in delivery groups, not in application groups.

For information about where user lists are specified in a deployment, see Where user lists are specified.

Step 3. Applications

Good to know:

- By default, new applications you add are placed in a folder named **Applications**. You can specify a different folder. If you try to add an application and one with the same name already exists in that folder, you are prompted to rename the application you are adding. If you agree with the suggested unique name, the application is added with that new name. Otherwise, you must rename it yourself before it can be added. For details, see Manage application folders.
- You can change an application's properties (settings) when you add it, or later. See Change application properties. If you publish two applications with the same name to the same users, change the **Application name (for user)** property in Studio. Otherwise, users will see duplicate names in the Citrix Workspace app.
- When you add an application to more than one application group, a visibility issue can occur if you do not have sufficient permission to view the application in all of those groups. In such cases, either consult an administrator with greater permissions or have your scope extended to include all the groups to which the application was added.

Select the **Add** dropdown to display the application sources.

- **From Start menu:** Applications that are discovered on a machine in the selected delivery groups. When you select this source, a new page launches with a list of discovered applications. Select the check boxes of applications to add, and then select **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This source cannot be selected if you selected any of the following:

- Application groups that have no associated delivery groups.
- Application groups with associated delivery groups that contain no machines.
- A delivery group containing no machines.

- **Manually:** Applications located in the site or elsewhere in your network. When you select this source, a new page launches where you type the path to the executable, working directory, optional command line arguments, and display names for administrators and users. After entering this information, select **OK**.
- **Existing**: Applications previously added to the site. When you select this source, a new page launches with a list of discovered applications. Select the check boxes of applications to add and then select **OK**. This source cannot be selected If the site has no applications.
- **Application packages:** Applications in App-V, MSIX, MSIX app attach, or FlexApp application packages. When you select this source, the **Add Applications from Packages** page launches. Select an application package source, select the applications you want to add from the resulting display, and then select **OK**

  NOTE:

  To publish MSIX or MSIX app attach apps, the delivery group's functional level must be 2106 or later. For FlexApp apps, the functional level must be 2206 or later. When a functional level requirement isn't met, the corresponding options in the **Application package source** dropdown list are dimmed. **Note:**

  On VDA version 2003 and later, publishing App-V packages from HTTP URLs is not supported. You cannot select those applications from the list.

As noted, certain entries in the **Add** dropdown will not be selectable if there is no valid source of that type. Sources that are incompatible are not listed at all (for example, you cannot add application groups to application groups, so that source is not listed when you create an application group).

Step 4. Scopes

This page appears only if you have previously created a custom scope. By default, the **All** scope is selected. For more information, see Delegated administration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 5. Summary

Enter a name for the application group. You can also (optionally) enter a description.

Review the summary information and then select **Finish**.

Manage application groups

Introduction

This article describes how to manage the application groups you created.

See Applications for information about managing applications in application groups or delivery groups, including how to:

- Add or remove applications in an application group.
- Change application group associations.

Managing application groups requires the delegated administration permissions of the Delivery Group Administrator built-in role. For details, see Delegated administration.

Enable or disable an application group

When an application group is enabled, it can deliver the applications that have been added to it. Disabling an application group disables each application in that group. However, if those applications are also associated with other enabled application groups, they can be delivered from those other groups. Similarly, if the application was explicitly added to delivery groups associated with the application group (in addition to being added to the application group), disabling the application group does not affect the applications in those delivery groups.

An application group is enabled when you create it. You cannot change this when you create the group.

1. From Studio, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. On the **Settings** page, select or clear the **Enable Application Group** check box.
4. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable or disable application session sharing between application groups

Session sharing between application groups is enabled when you create an application group. You cannot change this when you create the group. For more information, see Session sharing with application groups.

1. From Studio, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. On the **Settings** page, select or clear the **Enable application session sharing between Application Groups** check box.
4. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Disable application session sharing within an application group

Session sharing between applications in the same application group is enabled by default when you create an application group. If you disable application session sharing between application groups, session sharing between applications in the same application group remains enabled.

You can use the PowerShell SDK to configure application groups with application session sharing disabled between the applications they contain. In some circumstances this can be desirable. For example, you might want users to start non-seamless applications in full-size application windows on separate monitors.

When you disable application session sharing within an application group, each application in that group launches in a new application session. If a suitable disconnected session is available which is running the same application, it is reconnected. For example, if you launch Notepad, and there is a disconnected session with Notepad running, that session is reconnected instead of creating a new one. If multiple suitable disconnected sessions are available, one of the sessions is chosen to reconnect to, in a random but deterministic manner. If the situation reoccurs in the same circumstances, the same session is chosen, but the session is not necessarily predictable otherwise.

You can use the PowerShell SDK to either disable application session sharing for all applications in an existing application group, or to create an application group with application session sharing disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PowerShell cmdlet examples

To disable session sharing, use the Broker PowerShell cmdlets New-BrokerApplicationGroup or Set-BrokerApplicationGroup with the parameter SessionSharingEnabled set to False and the parameter SingleAppPerSession set to True.

- For example, to create an application group with application session sharing disabled for all applications in the group:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

- For example, to disable application session sharing between all applications in an existing application group:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

Considerations

- To enable the `SingleAppPerSession` property you must set the `SessionSharingEnabled` property to False. The two properties must not be enabled at the same time. The `SessionSharingEnabled` parameter refers to sharing sessions between application groups.
- Application session sharing works only for applications that are associated with application groups but are not associated with delivery groups. All applications that are associated directly with a delivery group share sessions by default.
- If an application is assigned to multiple application groups, make sure that the groups do not have conflicting settings. For example, one group with the option set to True, and another group's option set to False results in unpredictable behavior.

Rename an application group

1. From Studio, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Rename Application Group** in the action bar.
3. Specify the new unique name and then select **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add, remove, or change the priority of delivery group associations with an application group

An application group can be associated with delivery groups containing shared (not private) machines that can deliver applications.

You can also select delivery groups containing shared machines that deliver only desktops, if both of the following conditions are met:

- The delivery group contains shared machines and was created with a version earlier than 7.9.
- You have Edit Delivery Group permission.

The delivery group type is automatically converted to "desktops and applications" when the **Edit Application Group** dialog is committed.

1. From Studio, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. Select the **Delivery Groups** page.
4. To add delivery groups, select **Add**. Select the check boxes of available delivery groups. (Incompatible delivery groups cannot be selected.) When you finish your selections, select **OK**.
5. To remove delivery groups, select the check boxes of the groups you want to remove and then select **Remove**. Confirm the deletion when prompted.
6. To change the priority of delivery groups, select the check box of the delivery group and then select **Edit Priority**. Enter the priority (0 = highest) and then select **OK**.
7. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Add, change, or remove a tag restriction in an application group

Adding, changing, and removing tag restrictions can have unanticipated effects on which machines are considered for application launch. Review the considerations and cautions in Tags.

1. From Studio, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. Select the **Delivery Groups** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. To add a tag restriction, select **Restrict launches to machines with the tag** and then select the tag from the menu.
5. To change or remove a tag restriction, either select a different tag from the menu or remove the tag restriction by clearing **Restrict launches to machines with this tag**.
6. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Add or remove users in an application group

For detailed information about users, see Create application groups.

1. From Studio, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Edit Application Group** in the action bar.
3. Select the **Users** page. Indicate whether you want to allow all users in the associated delivery groups to use applications in the application group, or only specific users and groups. To add users, select **Add**, and then specify the users you want to add. To remove users, select one or more users and then select **Remove**.
4. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Add, change, or remove an application icon in an application group

Perform the following steps to add, change, or remove an application icon.

1. In the navigation pane, select **Applications**.
2. On the **All Applications** tab, select an application and then select **Properties**.

   To make changes at an application group level, navigate to the **Application Groups** tab, select an application in a group, and then select **Properties**.
3. Select the **Delivery** page and then select **Change**. The **Select Icon** window appears.
4. In the **Select Icon** window, do either of the following:

   - To add an icon, select **Add** and then browse to the icon.
   - To remove an icon, select it and then select **Remove**.
   - To change an icon, select it for the application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

- You cannot add an icon whose size is greater than 200 KB.
- You can add only .icon files.
- You cannot remove built-in icons.
- You cannot remove an icon of an application that is in use.

5. Select **OK** to apply changes and close the window.

Limitation

- The default icons for Windows desktops and applications have changed to generic PC desktop icons for version 2209 and later. This change is only applicable to desktops and applications that are pointing to the default icons deployed in versions earlier than 2209. If you upgrade to version 2209 or later and want to change the icons back to the Windows application default icon, run the following script using the Remote PowerShell SDK:

```
Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0
```

Change scopes in an application group

You can change a scope only if you have created a scope (you cannot edit the All scope). For more information, see Delegated administration.

1. From Studio, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group in the middle pane and then select **Edit Application Group** in the action bar.
3. Select the **Scopes** page. Select or clear the check box next to the scopes you want to change.
4. Select **Apply** to apply any changes you made and keep the window open, or select **OK** to apply changes and close the window.

Delete an application group

An application must be associated with at least one delivery group or application group. If deleting an application group will result in one or more applications no longer belonging to a group, you are

© 1997–2026 Citrix Systems, Inc. All rights reserved.

warned that deleting that group will also delete those applications. You can then confirm or cancel the deletion.

Deleting an application does not delete it from its original source. However, if you want to make it available again, you must add it again.

1. From Studio, select **Applications** in the left pane, and then select the **Application Groups** tab.
2. Select an application group and then select **Delete Group** in the action bar.
3. Confirm the deletion when prompted.

Organize application groups using folders

You can create folders to organize application groups for easy access.

Required roles

By default, you must have one of the following built-in roles to create and manage folders for application groups:

- Cloud Administrator
- Full Administrator
- Application Group Administrator

You can delegate management actions to other users by creating custom roles. The following table lists the permissions required for each action.

ACTION	REQUIRED PERMISSIONS
Create application group folders	Create Application Group Folder
Delete application group folders	Remove Application Group Folder
Move application groups folders	Move Application Group Folder
Rename application group folders	Edit Application Group Folder
Move application groups to folders	Edit Application Group Folder, Edit Application Group Properties

For more information, see Create and manage roles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create and manage folders

You can use the Actions bar or the right-click menu to create and manage application group folders. In addition, you can drag an application group or a folder to a desired location in the folder tree.

Good to know:

- You can nest folders up to five levels (*excluding* the default node folder).
- A folder can contain application groups and subfolders. You can delete a folder only if it and its subfolders don't contain application groups.
- All nodes in Studio (such as **Machine Catalogs**, **Delivery Groups**, **Applications**, and **Application Groups**) share the same folder tree in the back end. To avoid name conflicts when renaming or moving folders, use unique names for first-level folders across different nodes.

  If you create a folder using the `New-BrokerAdminFolder` SDK cmdlet and want it to appear under the **Application Groups** node, you must add the `ContainsApplicationGroups` metadata using the `Set-BrokerAdminFolderMetadata` cmdlet.

  Example:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplicationGroups -Value true
  ```

Remote PC Access

NOTE:

This article describes how to configure Remote PC Access using Studio. If you're using the Quick Deploy interface, follow the guidance in Remote PC Access in Quick Deploy.

Remote PC Access is a feature of Citrix Virtual Apps and Desktops™ that enables organizations to easily allow their employees to access corporate resources remotely in a secure manner. The Citrix platform makes this secure access possible by giving users access to their physical office PCs. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Remote PC Access eliminates the need to introduce and provide other

© 1997–2026 Citrix Systems, Inc. All rights reserved.

tools to accommodate teleworking. For example, virtual desktops or applications and their associated infrastructure.

Remote PC Access uses the same Citrix Virtual Apps and Desktops components that deliver virtual desktops and applications. As a result, the requirements and process of deploying and configuring Remote PC Access are the same as those required for deploying Citrix Virtual Apps and Desktops for the delivery of virtual resources. This uniformity provides a consistent and unified administrative experience. Users receive the best user experience by using Citrix HDX to deliver their office PC session.

The feature consists of a machine catalog of type **Remote PC Access** that provides the following functionality:

- Ability to add machines by specifying OUs. This ability facilitates the addition of PCs in bulk.
- Ability to add machines by using CSV files. This ability facilitates the addition of PCs in bulk in scenarios with OU structure restrictions.
- Automatic user assignment based on the user that logs into the office Windows PC. We support single user and multiple users assignments. By default, Citrix DaaS™ automatically assigns multiple users to the next unassigned machine. To restrict automatic assignment to a single user, navigate to **Settings > Site settings** and turn off the **Enable automatic assignment of multiple users for Remote PC Access** setting.

Citrix Virtual Apps and Desktops can accommodate more use cases for physical PCs by using other types of machine catalogs. These use cases include:

- Physical Linux PCs
- Pooled physical PCs (that is, randomly assigned, not dedicated)

NOTES:

For details on the supported OS versions, see the system requirements for the VDA for single-session OS and Linux VDA.

For on-premises deployments, Remote PC Access is valid only for Citrix DaaS Advanced or Premium licenses. Sessions consume licenses in the same way as other Citrix Virtual Desktops™ sessions. For Citrix Cloud, Remote PC Access is valid for Citrix DaaS and Workspace Premium Plus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Considerations

While all the technical requirements and considerations that apply to Citrix Virtual Apps and Desktops and Citrix DaaS in general also apply to Remote PC Access, some might be more relevant or exclusive to the physical PC use case.

IMPORTANT:

Windows 11 physical systems (and some running Windows 10) include virtualization-based security features that result in the VDA software's incorrectly detecting them as virtual machines. To mitigate this issue, you have the following options:

- Use the "/physicalmachine" option along with the "/remotepc" option as part of the VDA command-line installation
- Add the following registry value after the VDA is installed if the aforementioned option was not used `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - Name: ForceEnableRemotePC
  - Type: DWORD
  - Data: 1

Deployment considerations

While planning the deployment of Remote PC Access, make a few general decisions.

- You can add Remote PC Access to an existing Citrix Virtual Apps and Desktops and Citrix DaaS deployment. Before choosing this option, consider the following:
  - Are the current Delivery Controllers or Cloud Connectors appropriately sized to support the additional load associated with the Remote PC Access VDAs?
  - Are the on-premises site databases and database servers appropriately sized to support the additional load associated with the Remote PC Access VDAs?
  - Will the existing VDAs and the new Remote PC Access VDAs exceed the number of maximum supported VDAs per site?
- You must deploy the VDA to office PCs through an automated process. The following are two of options available:
  - Electronic Software Distribution (ESD) tools such as SCCM: Install VDAs using SCCM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Deployment scripts: Install VDAs using scripts.

- Review the Remote PC Access security considerations.

Machine catalog considerations

The type of machine catalog required depends on the use case:

- Remote PC Access machine catalog
    - Windows/Linux dedicated PCs
    - Windows/Linux dedicated multi-user PCs. This use case applies to physical office PCs that multiple users can access remotely in different shifts.
    - Pooled Windows/Linux PCs. This use case applies to physical PCs that multiple random users can access, such as computer labs.

Once you identify the type of machine catalog, consider the following:

- A machine can be assigned to only one machine catalog at a time.
- To facilitate delegated administration, consider creating machine catalogs based on geographic location, department, or any other grouping that eases delegating administration of each catalog to the appropriate administrators.
- When choosing the OUs in which the machine accounts reside, select lower-level OUs for greater granularity. If such granularity is not required, you can choose higher-level OUs. For example, in the case of Bank/Officers/Tellers, select **Tellers** for greater granularity. Otherwise, you can select **Officers** or **Bank** based on the requirement.
- Moving or deleting OUs after being assigned to a Remote PC Access machine catalog affects VDA associations and causes issues with future assignments. Therefore, make sure to plan accordingly so that OU assignment updates for machine catalogs are accounted for in the Active Directory change plan.
- You can choose OUs to add machines to the machine catalog in bulk. In some scenarios, doing that is not easy because of OU structure restrictions. Instead, you can add machines in bulk by using CSV files. That feature gives you more flexibility to bulk add machines. You can add only machines (for use with user auto-assignments) or add machines along with user assignments.
- Integrated Wake on LAN is available only with the **Remote PC Access** type machine catalog.

Linux VDA considerations

These considerations are specific to the Linux VDA:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Physical monitor blanking for Remote PC Access VDAs is available, but not for all Linux distributions. For the unsupported Linux distributions, use the Linux VDA on physical machines only in non-3D mode. Otherwise, due to limitations on NVIDIA's driver, the local screen of the PC cannot be blacked out and displays the activities of the session when HDX 3D mode is enabled. Showing this screen is a security risk.
- We recommend you use machine catalogs of type single-session OS for physical Linux machines.

Technical requirements and considerations

This section contains the technical requirements and considerations for physical PCs.

- The following are not supported:
  - KVM switches or other components that can disconnect a session.
  - Hybrid PCs, including All-in-One and NVIDIA Optimus laptops and PCs.
  - Dual boot machines.
- Connect the keyboard and mouse directly to the PC. Connecting to the monitor or other components that can be turned off or disconnected, can make these peripherals unavailable. If you must connect the input devices to components such as monitors, do not turn those components off.
- The PCs must be joined to an Active Directory Domain Services domain.
- Secure Boot is supported on Windows 10 only.
- The PC must have an active network connection. A wired connection is preferred for greater reliability and bandwidth.
- If using Wi-Fi, do the following:
  a. Set the power settings to leave the wireless adapter turned on.
  b. Configure the wireless adapter and network profile to allow automatic connection to the wireless network before the user logs on. Otherwise, the VDA does not register until the user logs on. The PC isn't available for remote access until a user has logged on.
  c. Ensure that the Delivery Controllers or Cloud Connectors can be reached from the Wi-Fi network.
- You can use Remote PC Access on laptop computers. Ensure that the laptop is connected to a power source instead of running on the battery. Configure the laptop power options to match the options of a desktop PC. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Disable the hibernate feature.

b. Disable the sleep feature.

c. Set the close lid action to **Do Nothing**.

d. Set the "press the power button" action to **Shut Down**.

e. Disable video card and NIC energy-saving features.

- Remote PC Access is supported on Surface Pro devices with Windows 10. Follow the same guidelines for laptops mentioned previously.
- If using a docking station, you can undock and redock laptops. When you undock the laptop, the VDA reregisters with the Delivery Controllers or Cloud Connectors over Wi-Fi. However, when you redock the laptop, the VDA doesn't switch to use the wired connection unless you disconnect the wireless adapter. Some devices provide built-in functionality to disconnect the wireless adapter upon establishing a wired connection. The other devices require custom solutions or third-party utilities to disconnect the wireless adapter. Review the Wi-Fi considerations mentioned previously.

  Do the following to enable docking and undocking for Remote PC Access devices:

  a. In the **Start** menu, select **Settings > System > Power & Sleep**, and set **Sleep** to **Never**.

  b. Under the **Device Manager > Network adapters > Ethernet adapter** go to **Power Management** and clear **Allow the computer to turn off this device to save power**. Ensure that **Allow this device to wake the computer** is checked.

- Multiple users with access to the same office PC see the same icon in Citrix Workspace app. When a user logs on to Citrix Workspace app, that resource appears as unavailable if already in use by another user.
- Install the Citrix Workspace app on each client device (for example, a home PC) that accesses the office PC.

Configuration sequence

This section contains an overview of how to configure Remote PC Access when using the **Remote PC Access** type machine catalog. For information on how to create other types of machine catalogs, see the Create machine catalogs.

1. On-premises site only - To use the integrated Wake on LAN feature, configure the prerequisites outlined in Wake on LAN.
2. If a new Citrix Virtual Apps and Desktops site was created for Remote PC Access:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Select the **Remote PC Access** site type.

b. On the **Power Management** page, choose to enable or disable power management for the default Remote PC Access machine catalog. You can change this setting later by editing the machine catalog properties. For details on configuring Wake on LAN, see Wake on LAN.

c. Complete the information on the **Users** and **Machine Accounts** pages.

Completing these steps creates a machine catalog named **Remote PC Access Machines** and a delivery group named **Remote PC Access Desktops**.

3. If adding to an existing Citrix Virtual Apps and Desktops site:

   a. Create a machine catalog of type **Remote PC Access** (Operating System page of the wizard). For details on how to create a machine catalog, see Create machine catalogs. Make sure to assign the correct OU so that the target PCs are made available for use with Remote PC Access.

   b. Create a delivery group to provide users access to the PCs in the machine catalog. For details on how to create a delivery group, see Create delivery groups. Make sure to assign the delivery group to an Active Directory group that contains the users that require access to their PCs.

4. Deploy the VDA to the office PCs.

   - We recommend using the single-session OS core VDA installer (`VDAWorkstationCoreSetup.exe`).
   - You can also use the single-session full VDA installer (`VDAWorkstationSetup.exe`) with the `/remotepc /physicalmachine` option, which achieves the same outcome as using the core VDA installer.
   - Consider enabling Windows Remote Assistance to allow help desk teams to provide remote support through Citrix Director. To do so, use the `/enable_remote_assistance` option. For details, see Install using the command line.
   - To be able to see logon duration information in Director, you must use the single-session full VDA installer and include the **Citrix User Profile Management WMI Plugin** component. Include this component by using the `/includeadditional` option. For details, see Install using the command line.
   - For information about deploying the VDA using SCCM, see Install VDAs using SCCM.
   - For information about deploying the VDA through deployment scripts, see Install VDAs using scripts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you successfully complete steps 2–4, users are automatically assigned to their own machines when they log in locally on the PCs.

5. Instruct users to download and install Citrix Workspace app on each client device that they use to access the office PC remotely. Citrix Workspace app is available from the Citrix download site or the application stores for supported mobile devices.

Features managed through the registry

CAUTION:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Sleep mode (minimum version 7.16)

To allow a Remote PC Access machine to go into a sleep state, add this registry setting on the VDA, and then restart the machine. After the restart, the operating system power saving settings are respected. The machine goes into sleep mode after the preconfigured idle timer passes. After the machine wakes up, it reregisters with the Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: DisableRemotePCSleepPreventer
- Type: DWORD
- Data: 1

Session management

By default, a remote user's session is automatically disconnected when a local user initiates a session on that machine (by pressing CTRL+ATL+DEL). To prevent this automatic action, add the following registry entry on the office PC, and then restart the machine.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: SasNotification
- Type: DWORD
- Data: 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, the remote user has preference over the local user when the connection message is not acknowledged within the timeout period. To configure the behavior, use this setting:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaMode
- Type: DWORD
- Data:
  - 1 - The remote user always has preference if he or she does not respond to the messaging UI in the specified timeout period. This behavior is the default if this setting is not configured.
  - 2 - The local user has preference.

The timeout for enforcing the Remote PC Access mode is 30 seconds by default. You can configure this timeout, but do not set it lower than 30 seconds. To configure the timeout, use this registry setting:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaTimeout
- Type: DWORD
- Data: number of seconds for timeout in decimal values

When a user wants to forcibly get the console access: The local user can press Ctrl+Alt+Del twice in a gap of 10 seconds to get local control over a remote session and force a disconnect event.

After the registry change and machine restart, if a local user presses Ctrl+Alt+Del to log on to that PC while it is in use by a remote user, the remote user receives a prompt. The prompt asks whether to allow or deny the local user's connection. Allowing the connection disconnects the remote user's session.

Wake on LAN

Remote PC Access supports Wake on LAN, which gives users the ability to turn on physical PCs remotely. This feature enables users to keep their office PCs turned off when not in use to save energy costs. It also enables remote access when a machine has been turned off inadvertently.

With the Wake on LAN feature, the magic packets are sent directly from the VDA running on the PC to the subnet in which the PC resides when instructed by the delivery controller. This allows the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

feature to work without dependencies on additional infrastructure components or third-party solutions for delivery of magic packets.

The Wake on LAN feature differs from the legacy SCCM-based Wake on LAN feature. SCCM-integrated Wake on LAN is an alternative Wake on LAN option for Remote PC Access that is only available with on-premises Citrix Virtual Apps and Desktops. For information on the SCCM-based Wake on LAN, see Wake on LAN – SCCM-integrated.

Limitation

Remote PC Access with the Wake on LAN feature does not support automatic power-on during peak times.

System requirements

The following are the system requirements for using the Wake on LAN feature:

- Control plane:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 or later
- Physical PCs:
  - VDA version 2009 or later
  - Windows 10 or Windows 11. For supportability details, see the VDA system requirements.
  - Wake on LAN enabled in BIOS/UEFI
  - Wake on LAN enabled in network adapter's properties within Windows configuration

Configure Wake on LAN

To configure Wake on LAN, you can use Studio or PowerShell.

Configure Wake on LAN using Studio

To create the Wake on LAN connection:

1. Navigate to the **Hosting** node on the left.
2. Select **Add Connection and Resources**.
3. In the **Connection** page of the wizard, provide the following:
   a. Connection type: Remote PC Wake on LAN
   b. Zone name: select the zone where the Remote PC Access catalog resides

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Connection name: enter a name for the Wake on LAN connection

4. Finalize the remaining steps in the Add Connection and Resources wizard.

To add the Wake on LAN connection to a Remote PC Access machine catalog:

1. If you are creating a new Remote PC Access machine catalog, you can add the connection on the **Machine Type** page of the Machine Catalog Setup wizard using the drop-down list.
2. If you want to add the Wake on LAN connection to an existing machine catalog:

   a. Navigate to the **Machine Catalogs** node on the left.

   b. Select the appropriate Remote PC Access machine catalog.

   c. Right-click on the machine catalog or select the **More** menu above.

   d. Select **Edit Machine Catalog**.

   e. In the **Power Management** page, select **Yes**.

   f. Select the appropriate connection from the drop-down list.

   g. Select **Save**.

NOTE:

The configuration of Wake on LAN through Studio is only available with Citrix DaaS at this time.

Configure Wake on LAN using PowerShell

To configure Wake on LAN using PowerShell:

1. Create the Remote PC Access machine catalog if you do not have one already.
2. Create the Wake on LAN host connection if you do not have one already.
3. Retrieve the Wake on LAN host connection's unique identifier.
4. Associate the Wake on LAN host connection with a machine catalog.

To create the Wake on LAN host connection:

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$hypHc.HypervisorConnectionUid

}
```

When the host connection is ready, run the following commands to retrieve the host connection's unique identifier:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

After you retrieve the connection's unique identifier, run the following commands to associate the connection with the Remote PC Access machine catalog:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

Design considerations

When you are planning to use Wake on LAN with Remote PC Access, consider the following:

- Multiple machine catalogs can use the same Wake on LAN host connection.
- For a PC to wake up another PC, both PCs must be in the same subnet and use the same Wake on LAN host connection. It does not matter if the PCs are in the same or different machine catalogs.
- Host connections are assigned to specific zones. If your deployment contains more than one zone, you need a Wake on LAN host connection in each zone. The same applies to machine catalogs.
- Magic packets are broadcasted using the global broadcast address 255.255.255.255. Ensure that the address is not blocked.
- There must be at least one PC turned on in the subnet - for every Wake on LAN connection - to be able to wake up machines in that subnet.

Operational considerations

The following are considerations for using the Wake on LAN feature:

- The VDA must register at least once before the PC can be woken up using the integrated Wake on LAN feature.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wake on LAN can only be used to wake up PCs. It does not support other power actions, such as restart or shut down.
- Magic packets are sent in one of the two ways:
  a. When a user tries to launch a session to their PC and the VDA is unregistered
  b. When an administrator manually sends a power on command from Studio or PowerShell
- Because the Delivery Controller is unaware of a PC's power state, Studio displays **Not Supported** under power state. The delivery controller uses the VDA registration state to determine whether a PC is on or off.

Troubleshoot

Monitor blanking not working

If the Windows PC's local monitor is not blank while there is an active HDX™ session (the local monitor displays what's happening in the session) it is likely due to issues with the GPU vendor's driver. To resolve the issue, give the Citrix Indirect Display driver (IDD) higher priority than the graphic card's vendor driver by setting the following registry value:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Name: CitrixIDD
- Type: DWORD
- Data: 3

For more details about display adapter priorities and monitor creation, see the Knowledge Center article CTX237608.

Session disconnects when you select Ctrl+Alt+Del on the machine that has session management notification enabled

The session management notification controlled by the **SasNotification** registry value only works when Remote PC Access mode is enabled on the VDA. If the physical PC has the Hyper-V role or any virtualization-based security features enabled, the PC reports as a virtual machine. If the VDA detects that it is running on a virtual machine, it automatically disables Remote PC Access mode. To enable Remote PC Access mode, add the following registry value:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: ForceEnableRemotePC

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Type: DWORD
- Data: 1

Restart the PC for the setting to take effect.

Diagnostic information

Diagnostic information about Remote PC Access is written to the Windows Application Event log. Informational messages are not throttled. Error messages are throttled by discarding duplicate messages.

- 3300 (informational): Machine added to catalog
- 3301 (informational): Machine added to delivery group
- 3302 (informational): Machine assigned to user
- 3303 (error): Exception

Power management

If power management for Remote PC Access is enabled, subnet-directed broadcasts might fail to start machines that are on a different subnet from the Controller. If you need power management across subnets using subnet-directed broadcasts, and AMT support is not available, try the Wake-up proxy or Unicast method. Ensure that those settings are enabled in the advanced properties for the power management connection.

The active remote session records the local touchscreen input

When the VDA enables Remote PC Access mode, the machine ignores the local touchscreen input during an active session. If the physical PC has the Hyper-V role or any virtualization-based security features enabled, the PC reports as a virtual machine. If the VDA detects that it is running on a virtual machine, it automatically disables Remote PC Access mode. To enable Remote PC Access mode, add the following registry setting:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: ForceEnableRemotePC
- Type: DWORD
- Data: 1

Restart the PC for the setting to take effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More resources

The following are other resources for Remote PC Access:

- Solution design guidance: Remote PC Access Design Decisions.
- Examples of Remote PC Access architectures: Reference Architecture for Citrix Remote PC Access Solution.

Standalone Citrix Secure Ticketing Authority (STA) service

The standalone Citrix Secure Ticketing Authority (STA) service enables you to have more control over the delivery of STA tickets in your environment.

The standalone Citrix STA service is installed on every Cloud Connector in a Resource Location by default. This service shifts STA ticketing from the Citrix Cloud™ ticketing service to the Cloud Connectors and standardizes ticketing operations across both normal and LHC modes. The standalone STA service reduces reliance on cloud services and reduces intermittent LHC events.

Standalone STA service scenarios and configuration requirements

The standalone STA service works in both normal and LHC mode when you are using the following:

- Citrix® StoreFront Cloud with On-premises Gateway: On-prem NetScaler® Gateways are configured for HDX proxy on a per-Resource Location basis. All Cloud Connectors in all the Resource Locations for which the NetScaler acts as an HDX proxy must be listed as STA servers in the NetScaler Gateway virtual server. If some STA servers in the Resource Location are missing, launches might fail.
- StoreFront™ with On-premises Gateway: All Cloud Connectors listed as STA servers on the StoreFront server must be listed as STA servers on the NetScaler Gateway virtual server. If some of the Cloud Connectors listed in StoreFront are not listed on the NetScaler Gateway virtual server, launches might fail.

Remove components

To remove components tht you installed (such as VDAs), Citrix® recommends using the Windows feature for removing or changing programs. Alternatively, you can remove components using the command line, or a script.

When you remove components, prerequisites are not removed, and firewall settings are not changed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you remove a VDA, the machine restarts automatically after the removal, by default.

Remove components using the Windows feature for removing or changing programs

From the Windows feature for removing or changing programs:

- To remove a VDA, select **Citrix Virtual Delivery Agent** \<*version*>, then right-click and select **Uninstall**. The installer launches and you can select the components to be removed.
- To remove the Universal Print Server, select **Citrix Universal™ Print Server**, then right-click and select **Uninstall**.

Remove a VDA using the command line

Run the command that was used to install the VDA: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, or `VDAWorkstationCoreSetup.exe`. See Install using the command line for syntax descriptions.

- To remove only the VDA or only the Citrix Workspace app, use the `/remove` and `/components` options.
- To remove the VDA and Citrix Workspace app, use the `/removeall` option.

For example, the following command removes the VDA and Citrix Workspace™ app from a multi-session OS machine.

```
VDAServerSetup.exe /removeall
```

For example, the following command removes the VDA but not Citrix Workspace app for Windows (if it is installed) from a single-session OS machine.

```
VDAWorkstationSetup.exe /remove /components vda
```

You can also remove a VDA using a script provided by Citrix. See Remove VDAs using the script.

User personalization layer

The user personalization layer feature for Citrix Virtual Apps and Desktops™ extends the capabilities of non-persistent machine catalogs to preserve users' data and locally installed applications across sessions. Powered by underlying Citrix App Layering technology, the user personalization layer feature supports Citrix Provisioning and Machine Creation Services (MCS) in a non-persistent machine catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You install the user personalization layer components alongside the Virtual Delivery Agent within the master image. A VHD file stores locally, user-installed applications. The VHD mounted on the image acts as the user's own virtual hard drive.

IMPORTANT:

You can deploy user personalization layers in Citrix Virtual Apps and Desktops, or App Layering user layers enabled in an image template, not both. Do not install the user personalization layer feature on a layer within App Layering.

This feature replaces Personal vDisk (PvD), while also providing a persistent workspace experience for users in a non-persistent, pooled, desktop environment.

To deploy the user personalization layer feature, install and configure it using the steps detailed in the article. Until then, the feature is not available.

Application support

Aside from the following exceptions, all applications that a user installs locally on the desktop are supported in the user personalization layer.

Exceptions

The following applications are the exception and are not supported on the user personalization layer:

- Enterprise applications, such as MS Office and Visual Studio.
- Applications that modify the network stack or hardware. Example: a VPN client.
- Applications that have boot level drivers. Example: a virus scanner.
- Applications with drivers that use the driver store. Example: a printer driver.

NOTE:

You can make printers available using Windows Group Policy Objects (GPOs).

Do *not* allow users to install any unsupported applications locally. Rather, install these applications directly on the master image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications that require a local user or administrator account

When a user installs an application locally, the app goes into their user layer. If the user then adds or edits a local user or group, the changes do not persist beyond the session.

IMPORTANT:

Add any required local user or group in the master image.

Requirements

The user personalization layer feature requires the following components:

- Citrix Virtual Apps and Desktops 7 1909 or later
- Virtual Delivery Agent (VDA), version 1912 or later
- Citrix Provisioning™, version 1909 or later
- Windows File Share (SMB), or Azure Files with on-prem AD authentication enabled

You can deploy the User personalization layer feature on the following Windows versions when the OS is deployed as single session. Support is limited to a single user on a single session.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, version 1607 or later
- Windows 10 Multi-Session (Azure Files supported)
- Windows Server 2016 (Azure Files supported)
- Windows Server 2019 (Azure Files supported)

For Citrix Virtual Apps and Desktops 7, use of Azure Files with User personalization layers is supported on Windows Server 2019, Windows Server 2016v, and Windows 10 client.

NOTE:

If you are using a server OS, only Server VDI is supported. For deployment details, see the Server VDI article.

User personalization layer supports just one user at a time per machine, and then the machine has to reboot to reset the disks. You cannot use user personalization layer with multi-session server operating systems, only with single-session server systems. User personalization layer works with non-persistent desktops only.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Uninstall the user personalization layer feature, if installed. Reboot the master image before installing the latest release.

Set up your file share

The user personalization layer feature requires Windows Server Message Block (SMB) storage. To create a Windows file share, follow the usual steps for the Windows operating system that you are on.

For more about using Azure Files with Azure-based catalogs, see Set up Azure Files storage for User personalization layers.

Recommendations

Follow the recommendations in this section for a successful user personalization layer deployment.

Microsoft System Center Configuration Manager (SCCM)

If you are using SCCM with the user personalization layer feature, follow the Microsoft guidelines for preparing your image in a VDI environment. Refer to this Microsoft TechNet article for more information.

User layer size

A user layer is a thin-provisioned disk that expands as space on the disk is used. The default size allowed for a user layer is 10 GB, the minimum we recommend.

NOTE:

During installation, if the value is set to zero (0), the default user layer size is set to 10 GB.

If you want to change the user layer size, you can enter a different value for the **User Layer Size** Studio policy. See **Step 5: Create delivery group custom policies**, under **Optional: Click Select next to User Layer Size in GB.**

Tools for overriding the User Layer Size (Optional)

You can override the User Layer Size by using a Windows tool to define a quota on the user layer file share.

Use one of the following Microsoft quota tools to set a hard quota on the user layer directory named **Users**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- File Server Resource Manager (FSRM)
- Quota Manager

NOTE:

Increasing the quota affects new user layers and expands existing ones. Decreasing the quota only affects new user layers. Existing user layers never decrease in size.

Deploy a User personalization layer

When deploying the user personalization feature, you define the policies within Studio. You then assign the policies to the delivery group bound to the machine catalog, where the feature is deployed.

If you leave the master image with no user personalization layer configuration, the services remain idle and do not interfere with authoring activities.

If you set the policies in the master image, the services attempt to run and mount a user layer within the master image. The master image would exhibit unexpected behaviors and instability.

To deploy the user personalization layer feature, complete the following steps in this order:

- Step 1: Verify availability of a Citrix Virtual Apps and Desktops environment.
- Step 2: Prepare your master image.
- Step 3: Create a machine catalog.
- Step 4: Create a delivery group.
- Step 5: Create delivery group custom policies.

NOTE:

Logging on for the first time after upgrading Windows 10 on the image takes longer than usual. The user's layer needs to update for the new version of Windows 10, which then increases logon time.

Step 1: Verify that the Citrix Virtual Apps and Desktops environment is available

Be sure that your Citrix Virtual Apps and Desktops environment is available to use with this new feature. For setup details, see Install and configure Citrix Virtual Apps and Desktops.

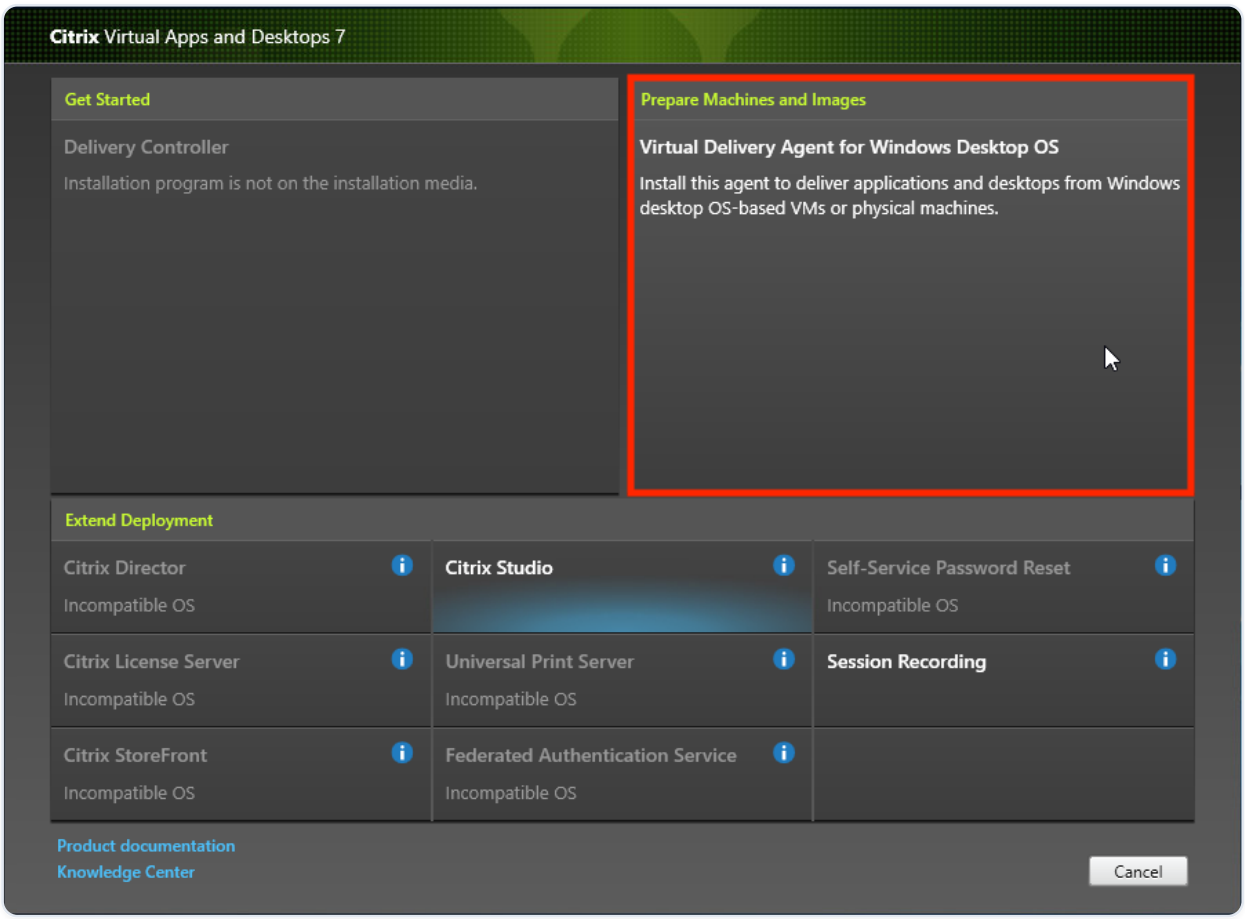
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Prepare your master image

To prepare your master image:

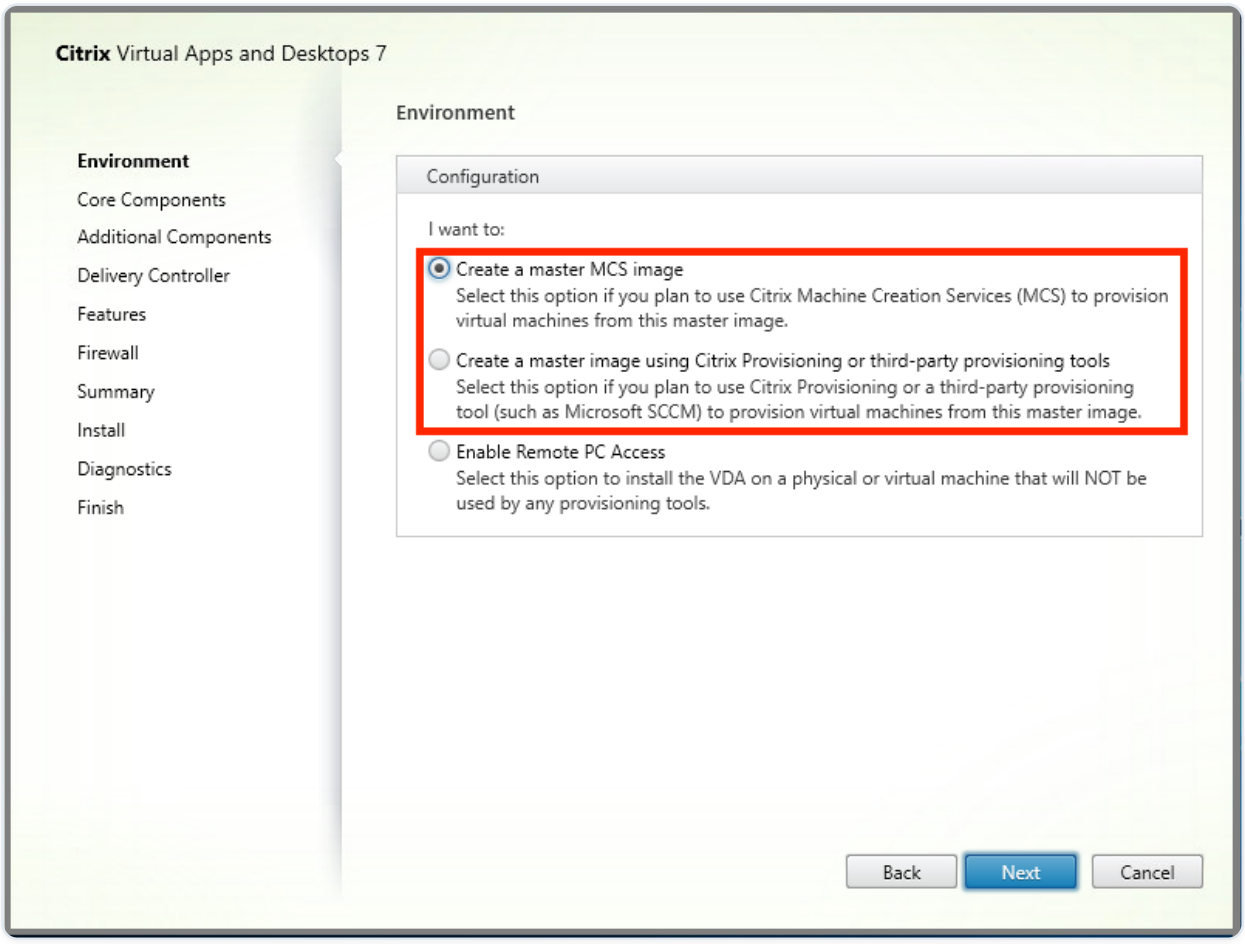
1. Locate the master image. Install your organization's enterprise applications and any other apps your users generally find useful.
2. If you are deploying Server VDI, follow the steps in the Server VDI article. Be sure to include the optional component, the **User personalization layer**. For details, see the Command-line options for installing a VDA.
3. If you are using Windows 10, install Virtual Delivery Agent (VDA) 1912 or later. If an older version of the VDA is already installed, uninstall the old version first. When installing the new version, be sure to select and install the optional component, the **Citrix User Personalization Layer**, as follows:

    a. Click the tile, **Virtual Delivery Agent for Windows Desktop OS**:



    a. **Environment:** Select either **Create a master MCS image** or **Create a master image using Citrix Provisioning or third-party provisioning tools**.

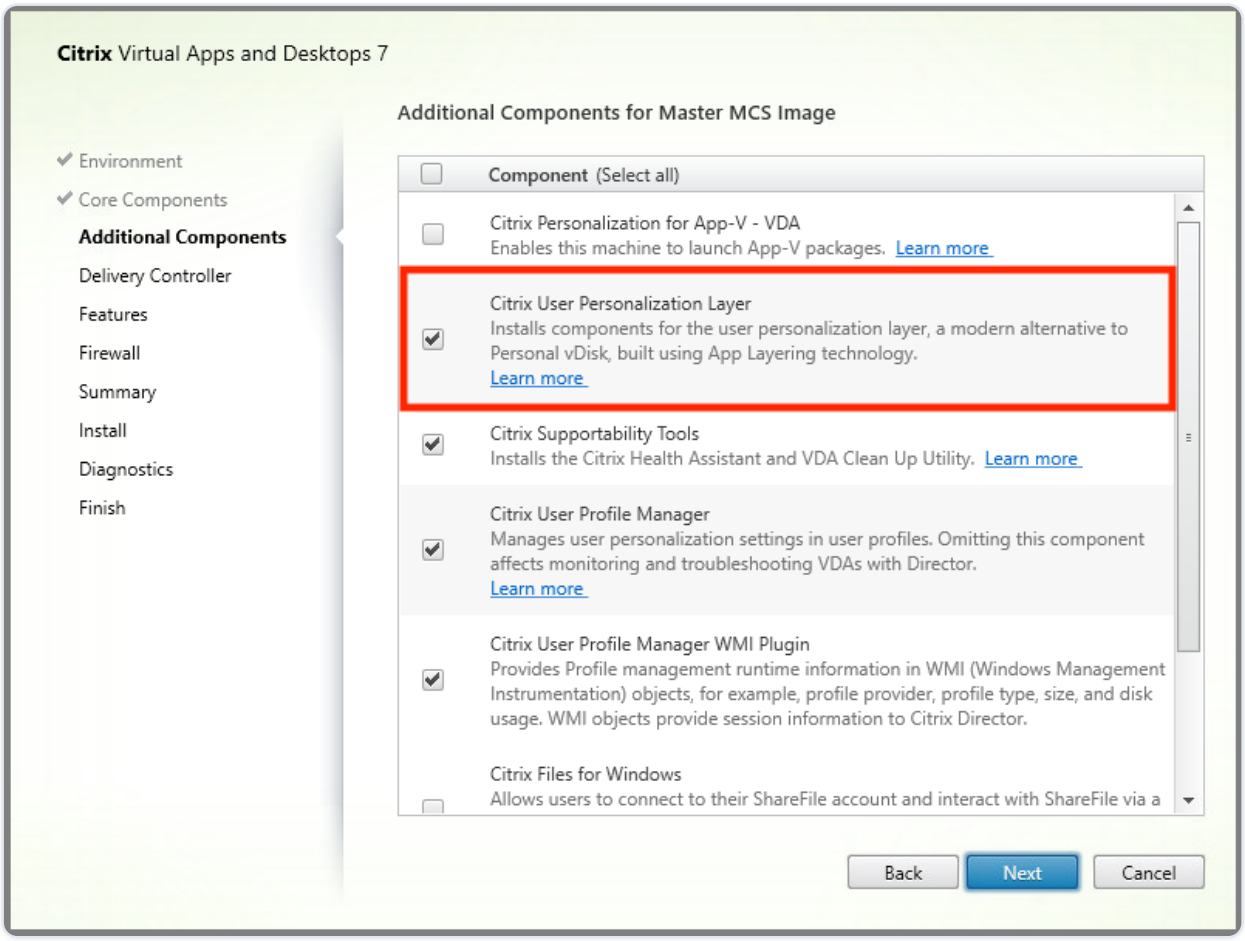
© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. **Core Components:** Click **Next**.

b. **Additional Components:** Check **Citrix User Personalization Layer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. Click through the remaining installation screens, configuring the VDA as needed, and click **Install**. The image reboots one or more times during installation.

4. Leave **Windows updates** disabled. The user personalization layer installer disables Windows updates on the image. Leave the updates disabled.

The image is ready for you to upload into Studio.

NOTE:

If you simply wish to upgrade the user personalization layer (UPL), you can do so with a newer version of UPL and the standalone package. You do not need to upgrade the VDA.

Step 3: Create a machine catalog

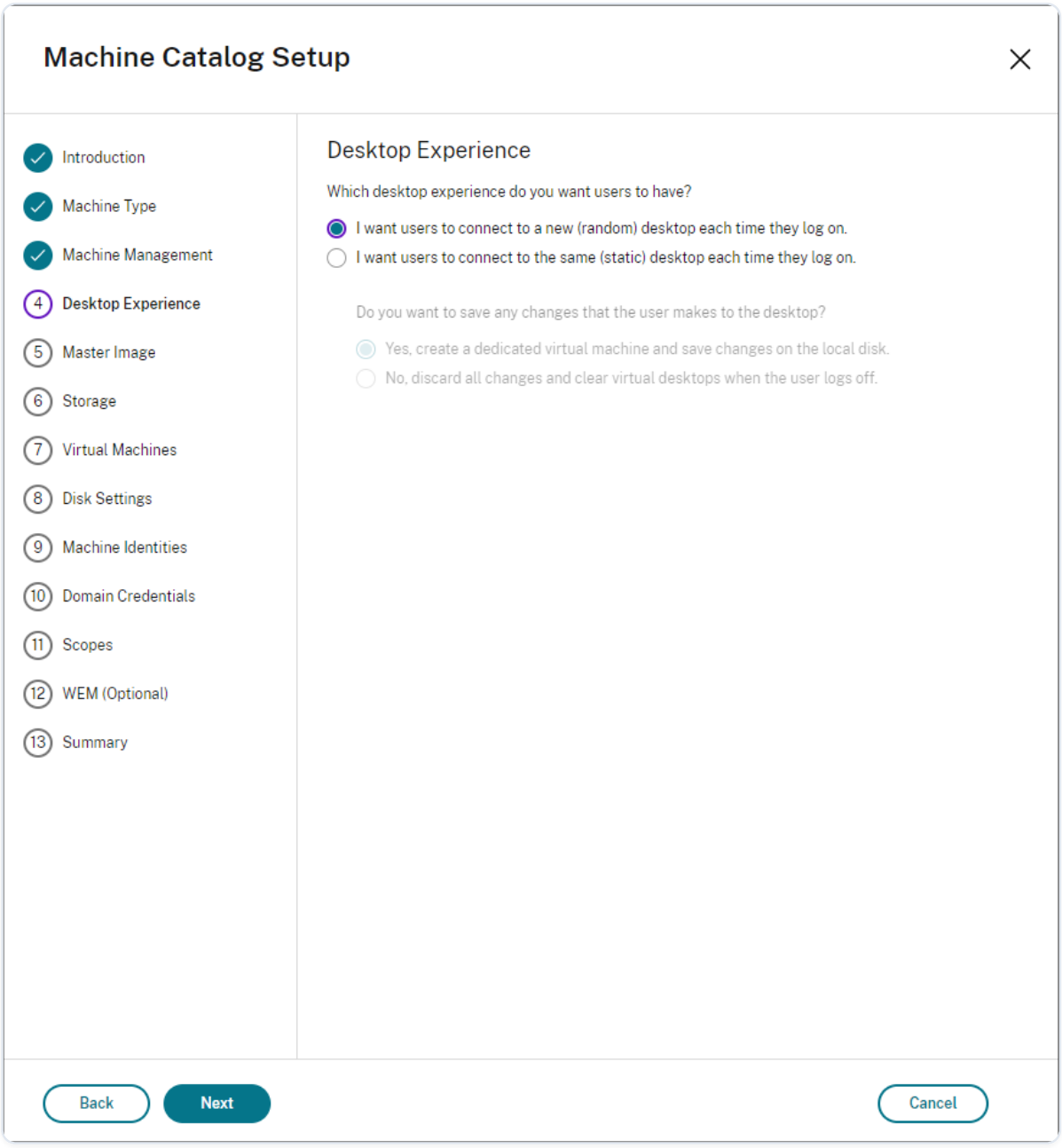
In Studio, follow the steps to create a machine catalog. Use the following options during catalog creation:

1. Select **Operating System** and set it to **Single session OS**.
2. Select **Machine Management** and set it to **Machines that are power managed**. For example, virtual machines or blade PCs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

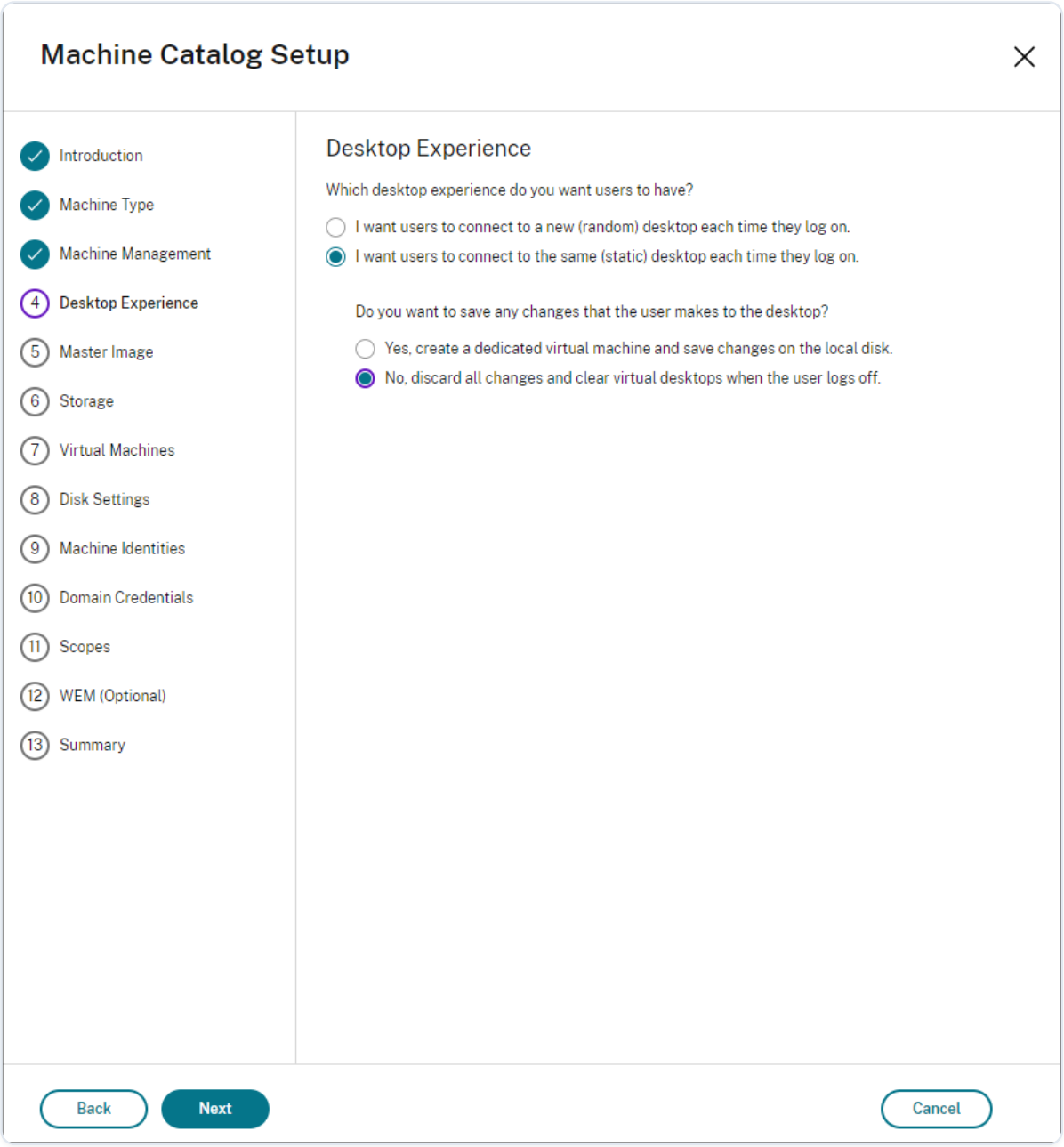
3. Select **Desktop Experience** and set it to either **pooled-random** or **pooled-static** catalog type, as in the following examples:

   - **Pooled-random:**



   - **Pooled-static:** If you select pooled-static, configure desktops to discard all changes and clear virtual desktops when the user logs off, as shown in the following screenshot:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

User personalization layer does not support pooled-static catalogs configured to use Citrix Personal vDisk or assigned as dedicated virtual machines.

4. If you are using MCS, select **Image** and the snapshot for the image created in the previous section.
5. Configure the remaining catalog properties as needed for your environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 4: Create a delivery group

Create and configure a **delivery group**, including machines from the machine catalog you created. For details, see the Create Delivery Groups.

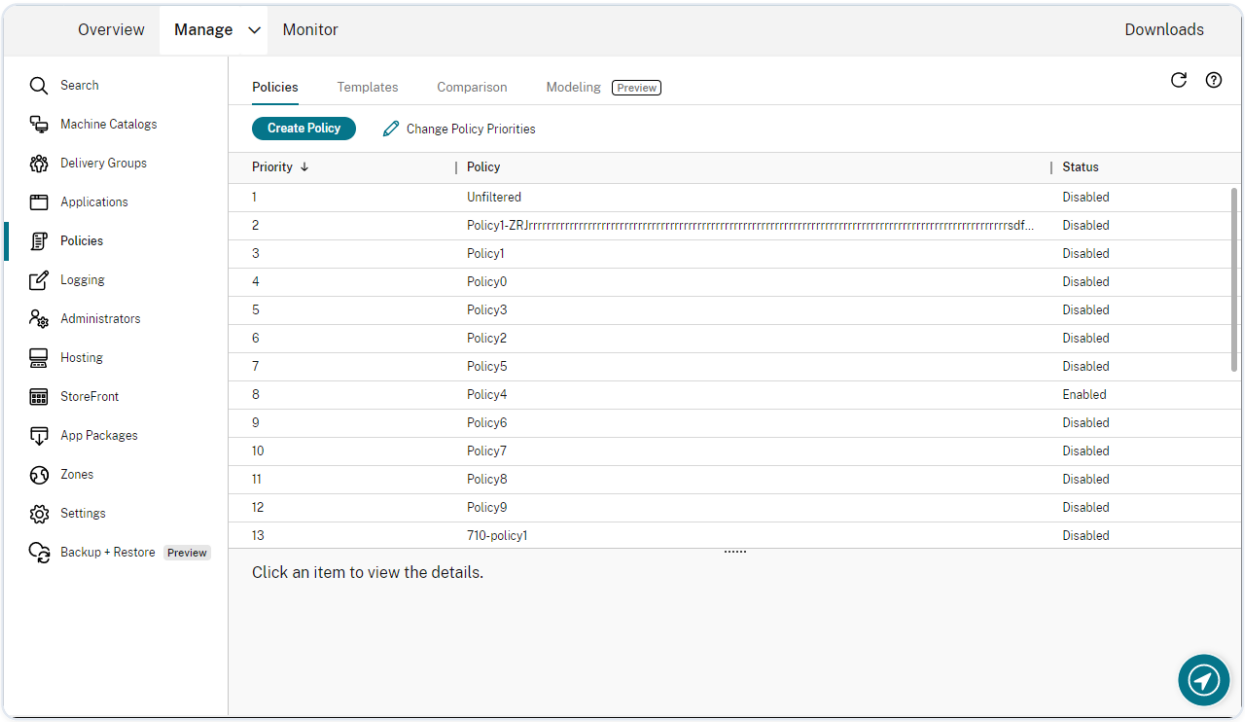
Step 5: Create delivery group custom policies

To enable mounting of user layers within the Virtual Delivery Agents, you use the configuration parameters to specify:

- Where on the network to access the user layers.
- How large to permit the user layer disks to grow.

To define the parameters as custom Citrix policies in Studio and assign them to your delivery group.

1. Sign in to Studio and select **Policies** in the left pane:



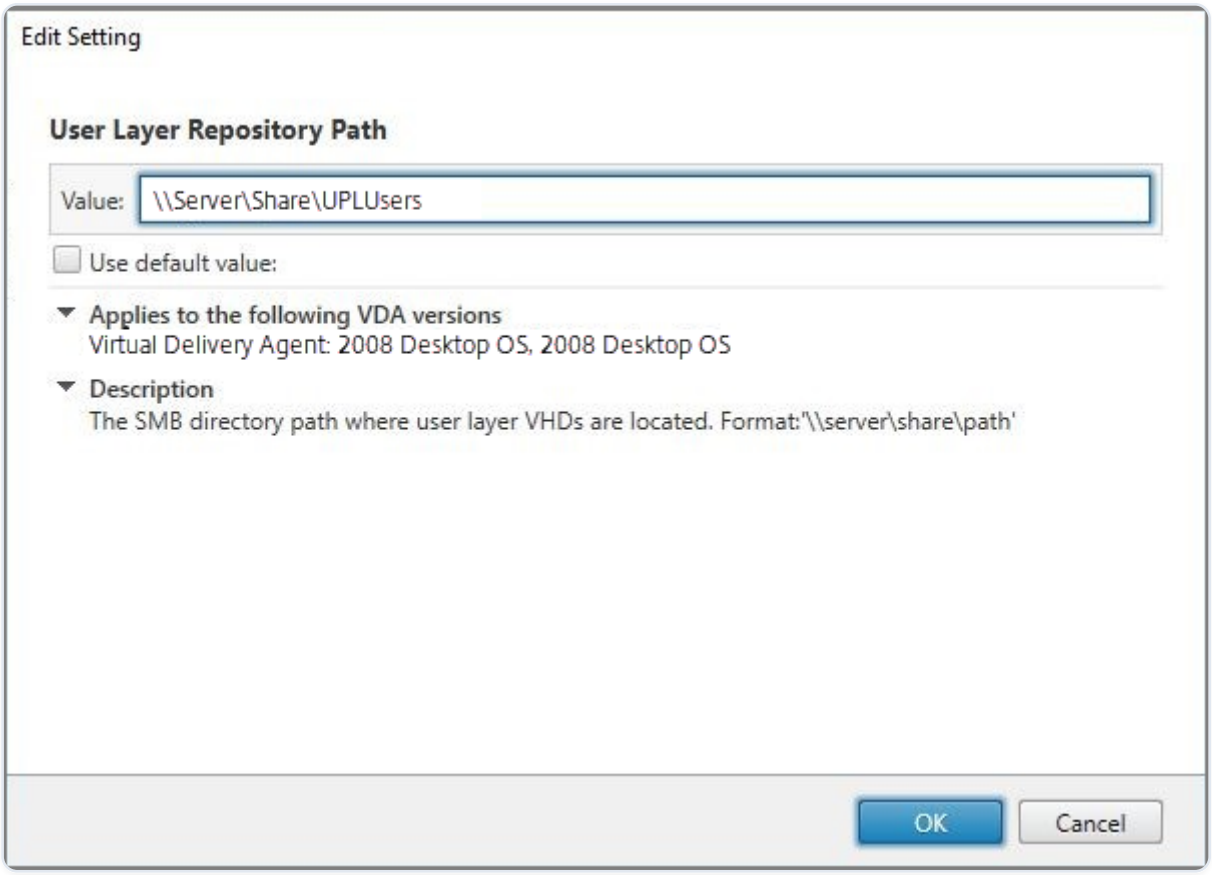
2. Select **Create Policy** in the action bar. The Create Policy window appears.
3. Type 'user layer' into the search field. The following three policies appear in the list of available policies:
    - User Layer Exclusions
    - User Layer Repository Path
    - User Layer Size GB

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Increasing the size affects new user layers and expands existing user layers. Decreasing the size only affects new user layers. Existing user layers never decrease in size.

4. Mark the check box next to **User Layer Repository Path** and click **Edit**. The Edit Setting window appears.
5. Enter a path in the **Value** field, and click **Save**:
   - **Path format:** `\\server-name-or-address\share-name\folder`
   - **Path example:** `\\Server\Share\UPLUsers`
   - **Resulting paths example:** For a user named **Alex** in **CoolCompanyDomain**, the path would be: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

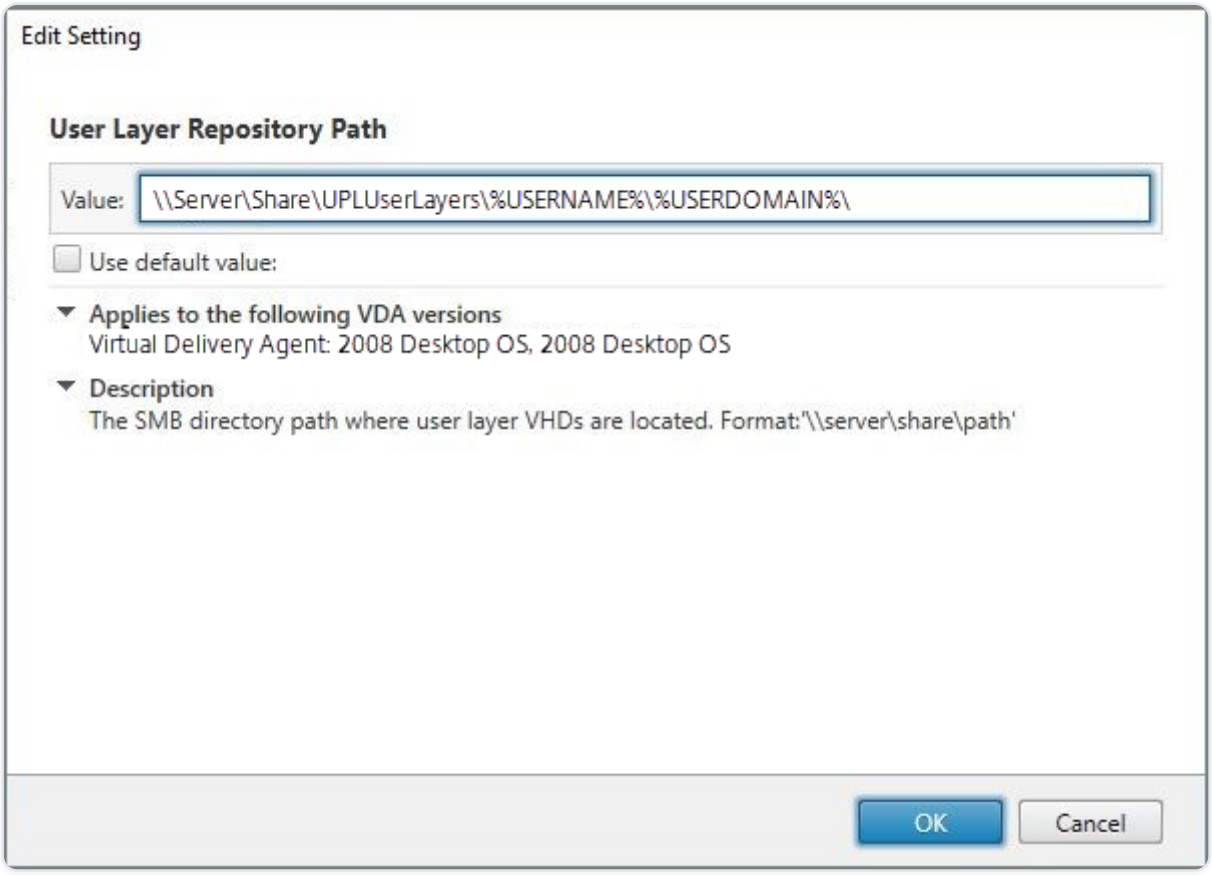


You can customize the path using the `%USERNAME%` and `%USERDOMAIN%` variables, machine environment variables, and Active Directory (AD) attributes. When expanded, these variables result in explicit paths.

Example of environment variables:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Path format:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Path example:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **Resulting paths example:** For a user named **Alex** in **CoolCompanyDomain**, the path would be: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

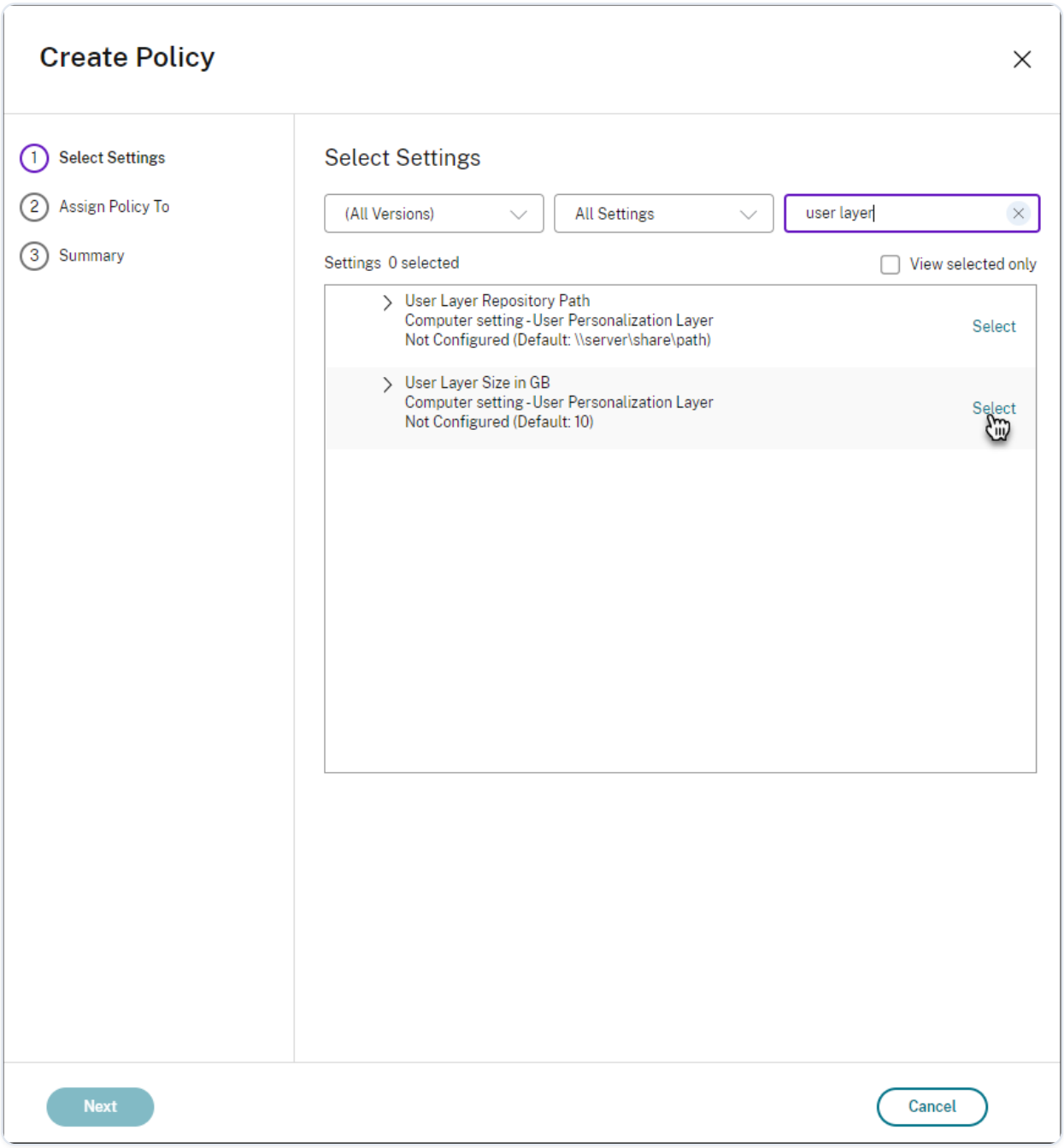


Example of custom AD attributes:

- Path format: `\\Server-name-or-address\share-name\AD-attribute`
- Path example: `\\Server\share#sAMAccountName#`
- Resulting paths example: `\\Server\share\JohnSmith` (if #sAMAccountName# resolves to JohnSmith for the current user)

6. Optional: Mark the check box next to **User Layer Size in GB** and click **Edit**:

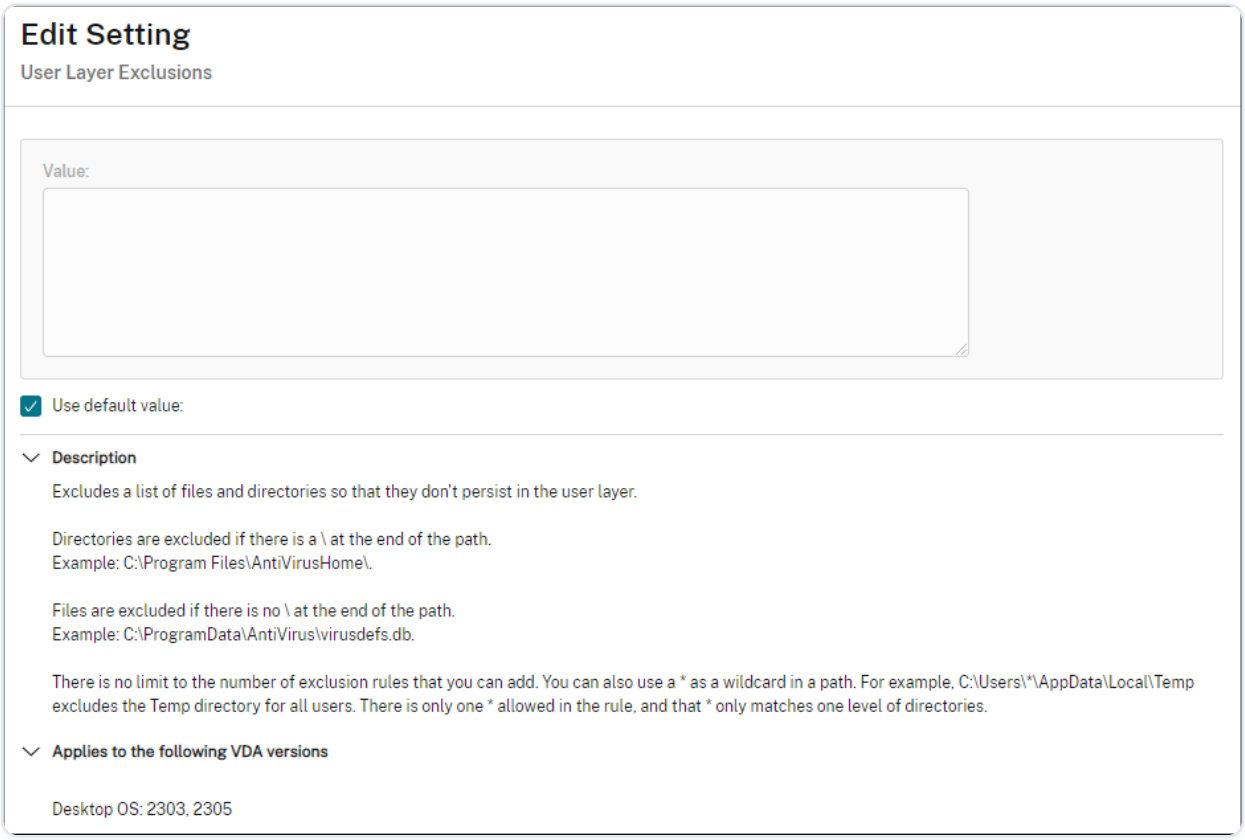
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The Edit Settings window appears.

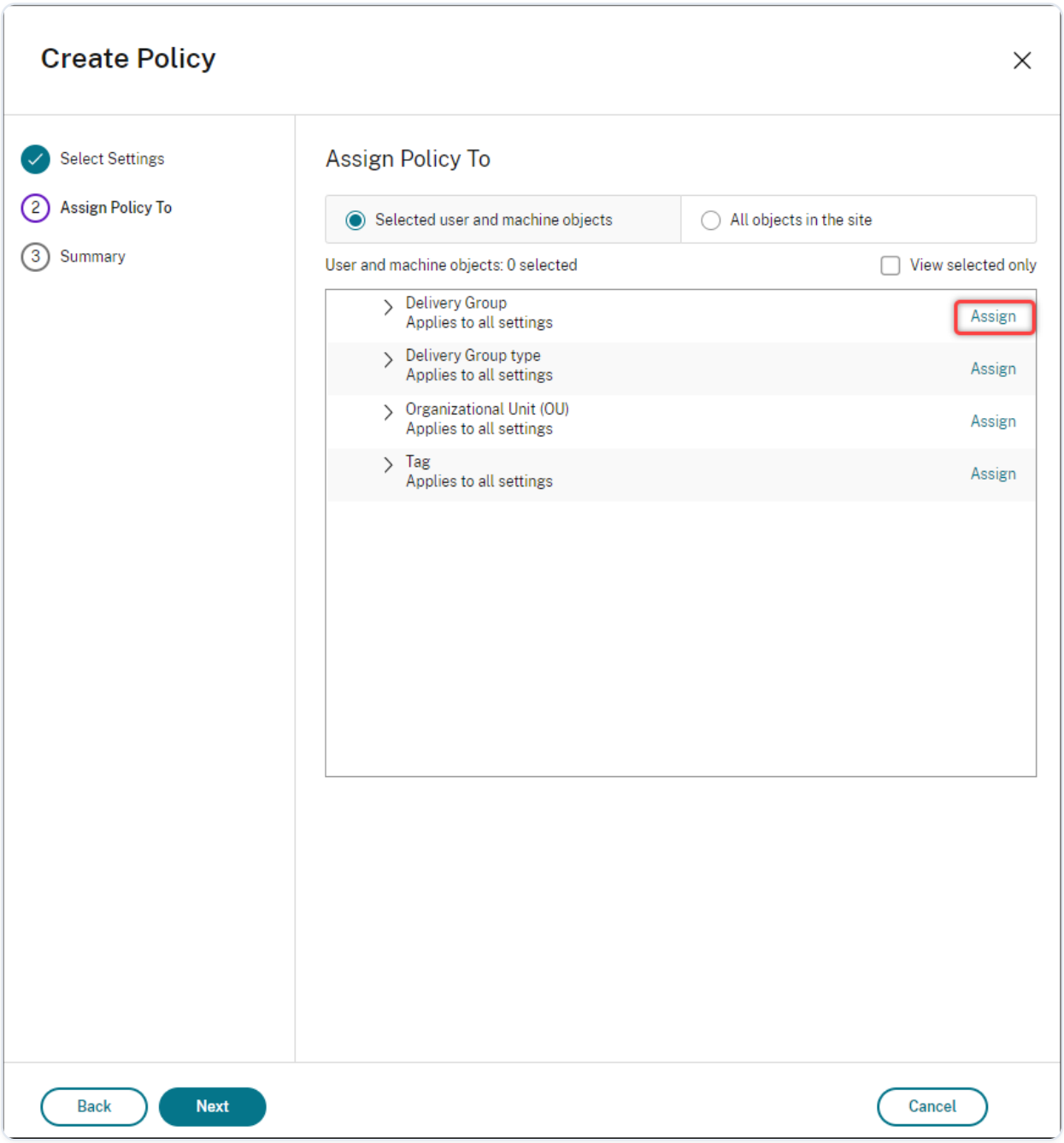
7. Optional: Change the default value of **10 GB** to the maximum size that each user layer can grow. Click **Save**.
8. Optional: Mark the check box next to **User Layer Exclusions** and click **Edit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

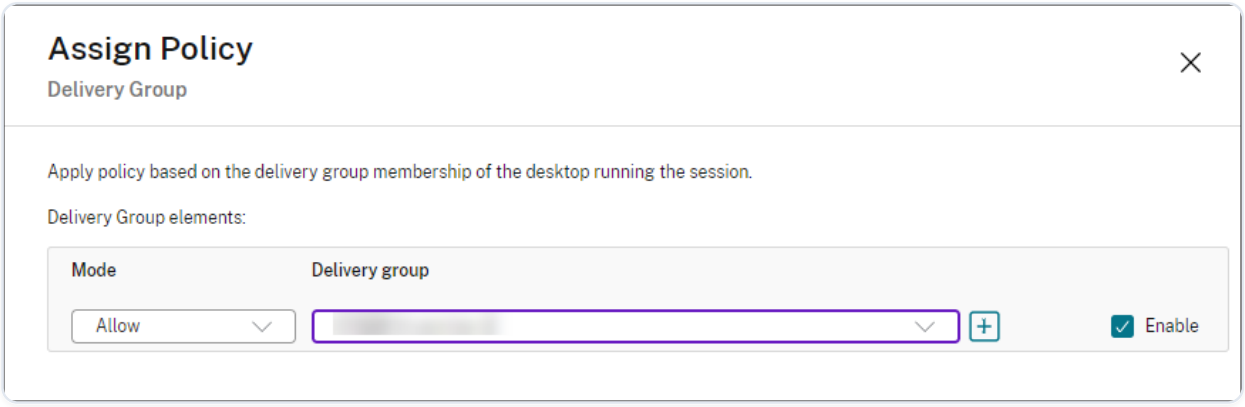


9. Optional: Specify the files and folders to exclude, then click **Save**. For more information, see the Citrix App Layering documentation.
10. Click **Next** to configure users and machines to which you want to assign. Click the **Delivery Group Assign** link highlighted in this image:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

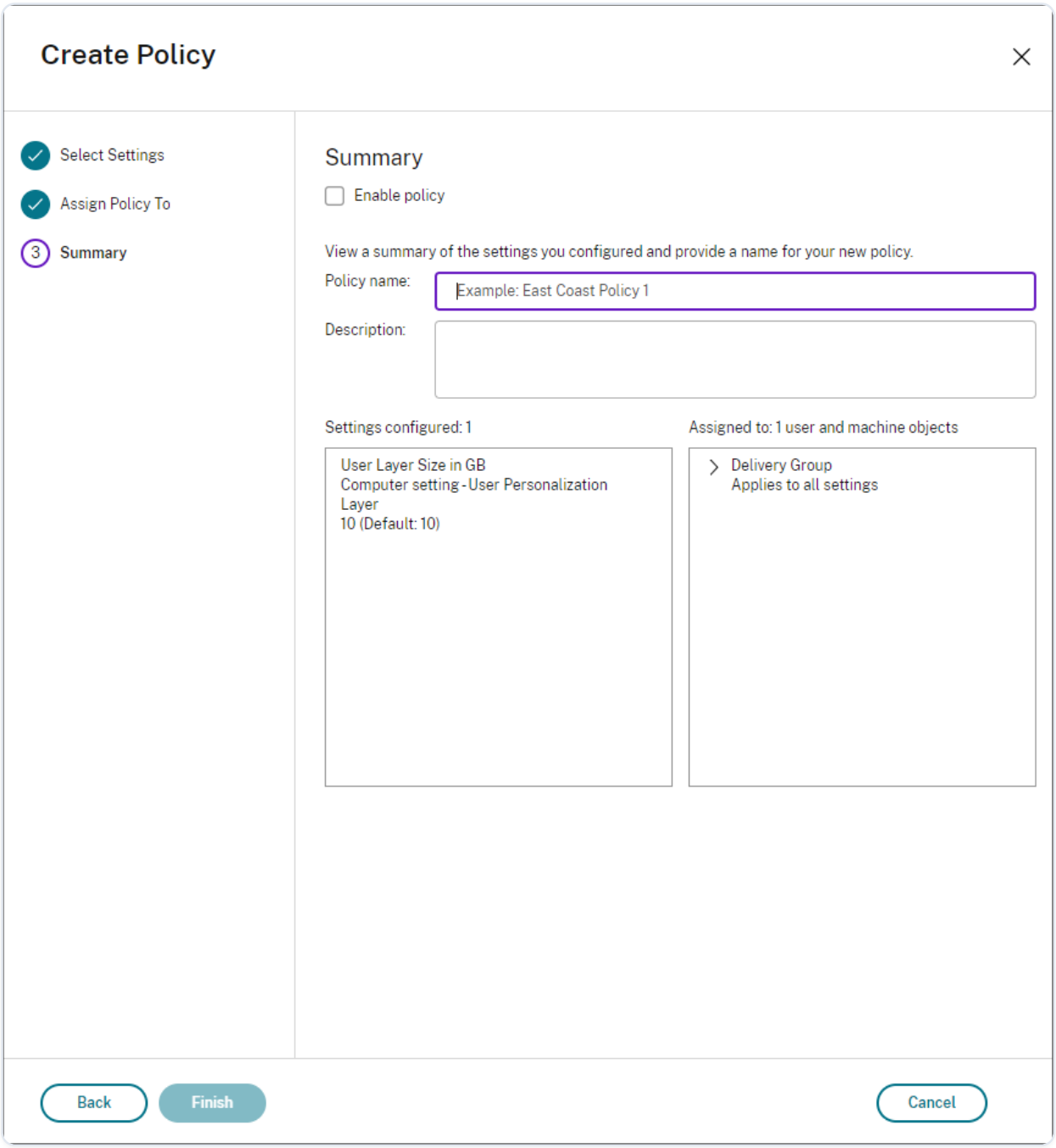


11. In the **Delivery Group** menu, select the delivery group created in the previous section. Click **OK**.



12. Enter a name for the policy. Click the check box to enable the policy, and click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure security settings on the user layer folder

As a domain administrator, you can specify more than one storage location for your user layers. Create a `\Users` subfolder For each storage location (including the default location). Secure each location using the following settings.

SETTING NAME	VALUE	APPLY TO	
Creator Owner	Modify	Subfolders and Files only	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SETTING NAME	VALUE	APPLY TO	
Owner Rights	Modify	Subfolders and Files only	
Users or group	Create Folder/ Append Data; Traverse Folder/ Execute File; List Folder/Read Data; Read Attributes	Selected Folder Only	
System	Full Control	Selected Folder, Subfolders, and Files	
Domain Admins, and selected Admin group	Full Control	Selected Folder, Subfolders, and Files	

User layer messages

When a user is unable to access their user layer, they receive one of these notification messages.

- **User Layer In Use**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`

- **User Layer Unavailable**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`

- **System not reset after user sign-out**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`

Log files to use when troubleshooting

The log file, ulayersvc.log, contains the output of the user personalization layer software where changes are logged.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

Limitations

Keep the following limitations in mind when installing and using the user personalization layer feature.

- Do *not* attempt to deploy the user personalization layer software on a layer within App Layering. Either deploy user personalization layers in Citrix Virtual Apps and Desktops, or enable user layers in an App Layering image template, not both. Either process produces the user layers you need.
- Do *not* configure the user personalization layer feature with persistent machine catalogs.
- Do *not* use Session hosts.
- Do *not* update the machine catalog with an image running a new OS install (even the same version of Windows 10). Best practice is to apply updates to the OS within the same master image used when creating the machine catalog.
- Do *not* use boot-time drivers, nor any other early boot personalization.
- Do *not* migrate PvD data to the user personalization layer feature.
- Do *not* migrate existing user layers from the full App Layering product to the user personalization layer feature.
- Do *not* change the user layer SMB path to access user layers created using a different master OS image.
- When a user logs out of a session and then logs in again, the new session runs on a different machine in the pool. In a VDI environment, Microsoft Software Center lists an application as **Installed** on the first machine, but shows it as **Unavailable** on the second machine.

  To find out the true status of the application, instruct the user to select the application in the Software Center and click **Install**. SCCM then updates the status to the true value.
- Software Center occasionally stops immediately after launching within a VDA that has the user personalization layer feature enabled. To avoid this issue, follow Microsoft's recommendations for Implementing SCCM in a XenDesktop VDI environment. Also, make sure that the `ccmexec` service is running before you start the Software Center.
- In Group Polices (Computer Settings), User layer settings override settings applied to the master image. Therefore, the changes you make in Computer Settings using a GPO are not always present for the user on the next session login.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To get around this issue, create a User Logon Script that issues the command:

```
gpupdate /force
```

For example, one customer set the following command to run at each user login:

```
gpudate /Target:Computer /force
```

For best results, apply changes to Computer Settings directly on the user layer, after the user has logged in.

- A domain user account must not be the last user to have logged in to a master image. Otherwise the machines provisioned from that image will have issues.
- Custom certificates do not persist when UPL is enabled in a pure Microsoft Entra environment, due to an underlying issue in Windows running on Azure. If Microsoft fixes this issue in a future enhancement, we will update this article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Backup or Migrate your configuration

This feature helps you take a backup of your DaaS configurations. Backup along with the restore feature facilitates the migration of site information from on-premises to the cloud or from one cloud site to another with ease. It also facilitates immediate rebounding of a site in times of emergencies.

You can use the following methods to take backups:

1. Backup + Restore
    a. Integrated with Studio.
2. Automated Configuration Tool (ACT)
    a. Powershell-based tool. Install the tool to use it. See Download Automated Configuration.

The backups can be used for:

1. Restoration
2. Migration

Citrix® recommends the following tools for the described scenarios.

Backup

ENVIRONMENT	USE CASE	RECOMMENDED TOOL	SPECIAL CONSIDERATIONS	LINK
DaaS and on-premises	On-demand and scheduled backups	Backup + Restore	Citrix keeps the backup and the user can download it if needed	Backup and Restore using Studio
DaaS and on-premises	On-demand and schedule backups	ACT	User keeps the backup	Backup and Restore using Automated

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ENVIRONMENT	USE CASE	RECOMMENDED TOOL	SPECIAL CONSIDERATIONS	LINK
				Configuration Tool

Migration

ENVIRONMENT	USE CASE	RECOMMENDED TOOL	SPECIAL CONSIDERATIONS	LINK
On-premise to cloud	Migrate one on-premises site to DaaS	ACT		Migrate from on-premises to cloud
	Consolidate multiple on-premises sites to one DaaS site	ACT	Site merging	Merge multiple on-premises sites to a single cloud site
On-premise to on-premise	Migrate one on-premises site to another on-premises site	ACT		POC Guide:Automated Configuration Tool- On-premises to On-premises migration
	Consolidate multiple on-premises sites to another on-premise site	ACT	Site merging	POC Guide:Automated Configuration Tool On-premises to On-premises migration

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ENVIRONMENT	USE CASE	RECOMMENDED TOOL	SPECIAL CONSIDERATIONS	LINK
				Merge multiple on-premises sites to a single cloud site
Cloud to cloud	Migrate one DaaS site to another DaaS site	ACT		Migrate from cloud to cloud
Consolidate multiple DaaS sites to one DaaS site	Site merging	ACT		Migrate from cloud to cloud
				Migrate multiple on-premises sites to a single cloud site

Backup and Restore configuration

This feature allows administrators to take a backup of your cloud configurations. It ensures that there is always a copy of your Citrix® configurations available, ready to be used. Backup along with the restore feature facilitates the migration of site information from on-premises to the cloud or from one cloud site to another with ease. If accidental changes arise, choose a backup, and select restore, and with a few clicks, you're up and running again. You can also choose to backup and restore specific components.

The feature allows you to back up and restore the following:

- Tags
- AdminRoles
- AdminScopes
- HostConnections

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You can now backup Host Connections in DaaS. Secrets must be entered each time. A pre-import check mode is performed to only ask secrets for those Host Connections that are imported or updated.

- StoreFront™
- Delivery groups
- ApplicationGroups
- Applications
- AppVIsolationGroups
- AppLibPackageDiscovery
- GroupPolicies
- UserZonePreference
- Manually provisioned or PVS provisioned machine catalogs
- Admin folders
  - Application folders
  - Delivery group folders
  - Machine catalog folders
- SiteSettings

IMPORTANT:

Make sure that you follow the order of the list given above to restore different components. For example, if you want to restore Applications, Delivery groups, and Group policies, you must follow the order:

- Delivery groups
- Applications
- Group policies.

Note:

You cannot back up or restore MCS machine catalogs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type of backups

Use the following options to perform backups according to your requirements:

- **On-demand**: Backs up site configurations in real time. This action backs up the current Citrix Cloud™ site configurations.
- **Scheduled**: Backs up site configurations at scheduled intervals. This recurs at the intervals mentioned.

NOTE:

Only administrators with full rights and cloud administrators can do on-demand or scheduled backups and restoration.

Backup and Restore using Studio

This article describes the actions that you can perform on the **Backup and Restore** node available in the left pane of your Manage DaaS console.

Backup and Restore allows the administrator to take backups from the Studio.

Create on-demand backups

1. Sign in to Citrix Cloud.
2. Click the **DaaS** tile.
3. From the left-menu, select **Backup and Restore**.
4. Within the **Backup and Restore** tab, click **Create backup**.
5. On the **Create backup** page, enter the notes, and click **Create backup**.

   A summary activity is displayed showing the backup components being backed up in the admin's name who triggers the back up.
6. After the backup completes successfully, it is listed as a line item under the **Backup and Restore** tab.
7. Select a particular backup to see more information on the backup in the **Details** tab.

To delete a backup, right-click a backup and click **Delete backup**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pin a backup

Citrix® stores the last 30 backups. When you create more than 30 backups, the system deletes old backups in the order they were created. For every new backup that is created in addition to the 30 backup limit, the system deletes the backup that was created first. Pin backup is used to prevent automatic deletion of a particular backup. You can pin up to 5 backups. In case there are pinned backups, we retain all pinned backups in addition to 30 backups that is at most, you can retain 35 backups – 30 non-pinned, and 5 pinned backups.

1. Right-click a backup to pin.

Create scheduled backups

Create a backup schedule that aligns with your organization's requirements to automate your backup and restore processes. Backups operate in the background at a frequency that you select (daily, weekly, monthly, or other suitable frequency).

1. Go to the schedule tab and select **Create Schedule**.
2. On the **Create schedule** page, enter the following:
    - **Enable this schedule**. Choose **yes** to enable this backup schedule.
    - **Name**. Enter a name for the backup schedule.
    - **Description**. Enter a description.
    - **Time zone**. Select the time zone of your choice.
    - **Frequency**. Select the frequency to run the backup.
    - **Repeats every**. Enter the number of days after which the schedule must be repeated.
    - **Start date**. Enter the start date.
    - **Begin backup at**. Enter the time when you want the backup to begin in a 24-hour format.
3. Select **Done**.

Limit scheduled backups

You can limit scheduled backups to one per day to avoid identical backups.

1. Go to the **Settings** tab of the **Backup and Restore** node.
2. Click **Change** in **Scheduled backups** box.
3. Switch the toggle to enable limit scheduled backups to one per day.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auto-pin scheduled backups

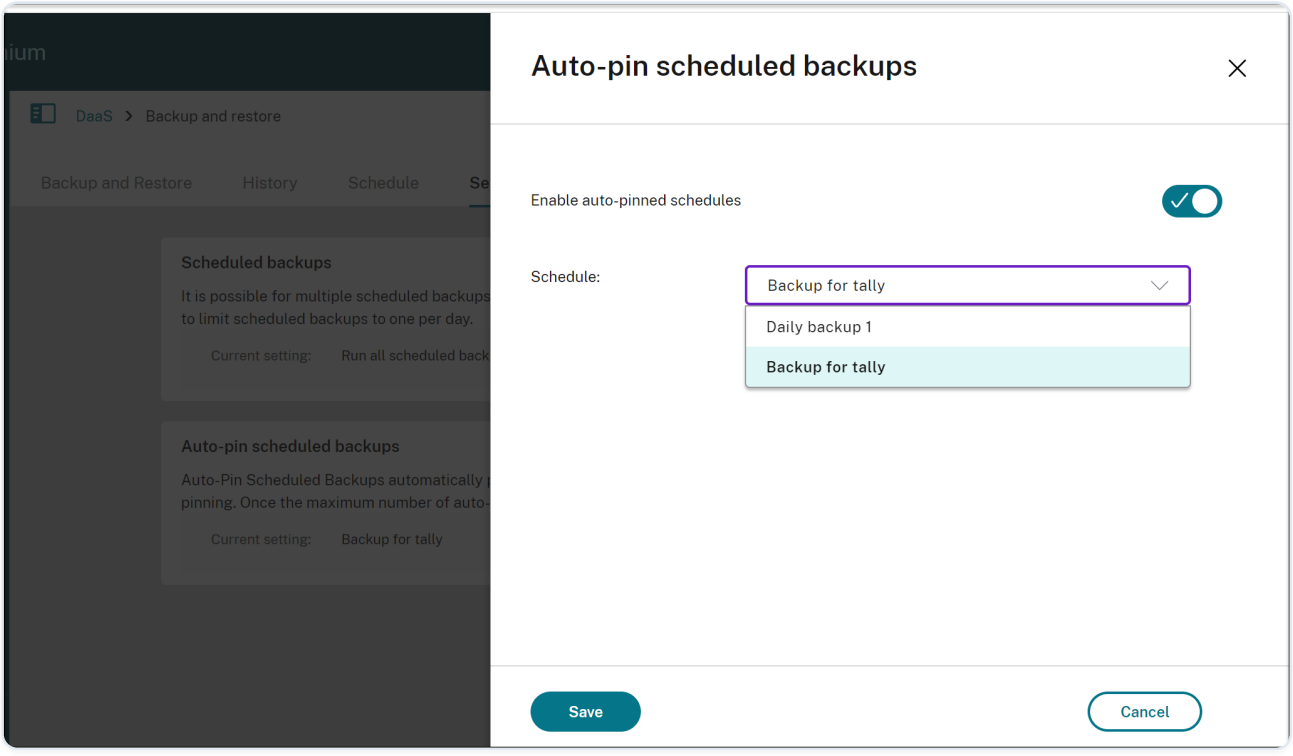
Auto-Pin scheduled backups automatically pins backups created by the selected schedule. Only one schedule can be selected for auto-pinning.

Using auto-pin scheduled backups you can retain a maximum of six scheduled backups. When the maximum limit is reached, the oldest auto-pinned backup is deleted.

NOTE:

Citrix stores up to six auto-pinned backups. The system deletes old backups in the order they were created after the sixth backup. For every new backup that is created in addition to the six backup limit, the system deletes the backup that was created first.

1. Go to the **Settings** tab of the **Backup and Restore** node.
2. Select a scheduled backup for auto-pinning.
3. Switch the toggle to enable auto-pinned schedules.
4. Select a schedule and click **Save**.



Restore

This feature allows the administrators to restore the site configurations from the backups. We allow you to restore one component at a time.

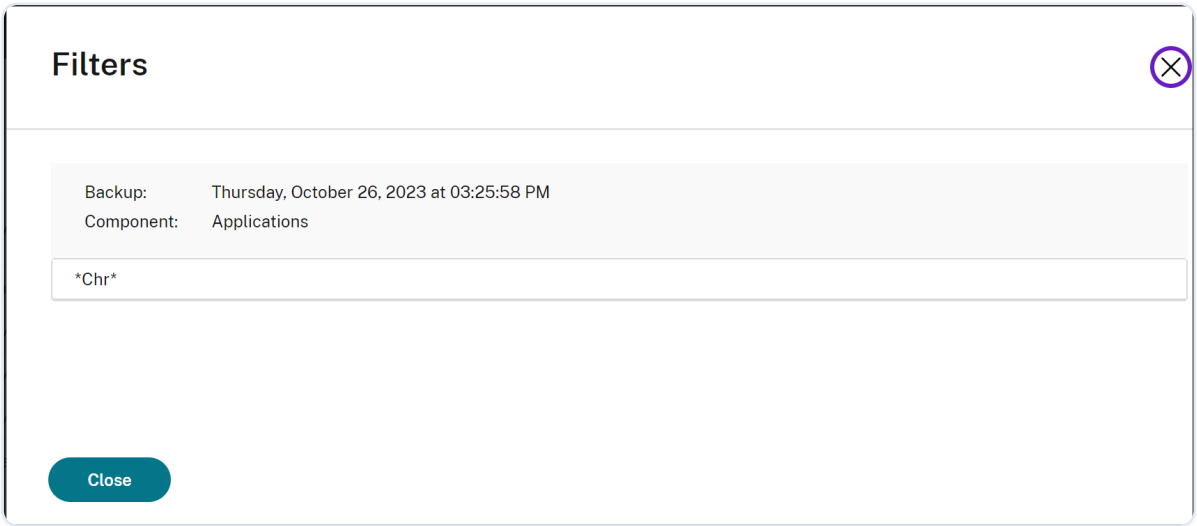
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Restoring only one component at a time ensures that there are no conflicts during restoration due to the dependencies between the components.
- The workflow for restoring host connections is different from other components as you would need to enter the secret every time you try to restore the host connection. After you click **Restore Backup**, you must see a dialog to enter the secret. For example, for Azure, enter the alphanumeric application secret used to create the connection.

1. Right-click a specific backup from the list and click **Restore Backup**.
2. On the **Restore Backup** window, enter the following:

   - **Components**: Select the components that you want to restore.
   - **Filters**: Specify the member names that you want to restore in a comma-separated list. For example, filtering for the word *chrome* restores only objects with the name chrome. Similarly, the phrase `chr` restores objects beginning with `chr`.

     To view the component members, select a backup and navigate to **Details > Components**. Select a component and click **View component members**.
   - **Check mode**: Choose **yes** to confirm what must be restored when an actual restore operation is done. This option pre-evaluates everything needed for a restore without actually triggering one. For example, it displays the list of applications that will be restored when the restore process is run for the applications component.

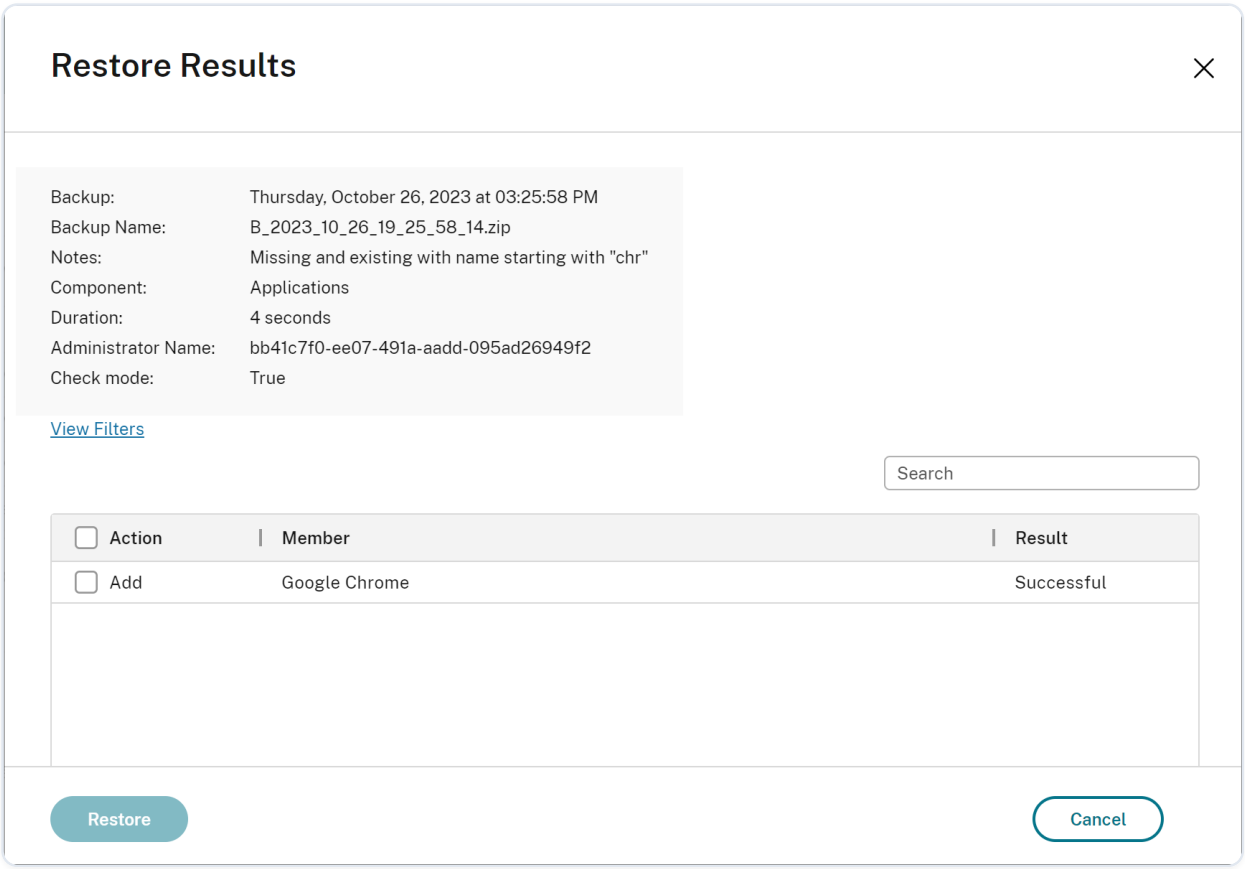
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Check mode does not run the actual restore. This option also does not check for any dependencies between the components. For optimal results, we recommend using the check mode on one component at a time.

- **Restore type**: Choose either one:
  - **Missing only**: Use this restore type to add components and members to a site. This option does not change the existing components and members even if the backup being restored has different configurations.
  - **Missing and updating existing**: Use this restore type to add and update components to a site. This option updates the existing components and members with the configurations of the backup if both have different configurations.
- **Notes**: Enter any notes.

3. Select **Restore**.



The restore results are listed in the **Restore** window after the restore action is completed. All restore actions are listed under the **History** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

History

You can track all the backup and restore actions in the **History** tab.

Under **Actions**, you can see all deleted backup and backup history.

To view details about a backup:

1. Go to the **History** tab.
2. Select a backup action and click **View details**.

The backup results give you the following details:

- Duration
- Notes
- Administrator name
- Components backed up

Use the search bar on the top right corner of the **History** page to search for a specific backup. For example: you can search for backups taken by a particular admin or taken on a particular day.

Backup and Restore using the Automated Configuration tool

Automated Configuration tool allows you to take on-demand and scheduled backups in the following environments:

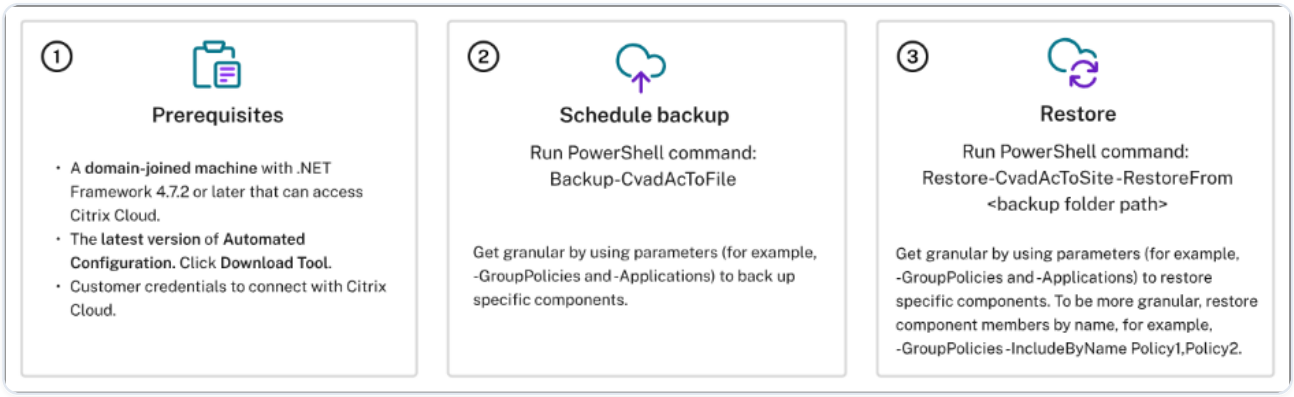
- Citrix Virtual Apps and Desktops™
- DaaS

Automated Configuration tool can be used for the following:

- Backup and restore (on-demand and scheduled backups)
- Migration (on-demand backups)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Automated Configuration tool for migration



Citrix Virtual Apps and Desktops

PREREQUISITES FOR BACKING UP YOUR CONFIGURATIONS

- All versions of Citrix Virtual Apps and Desktops.
- A machine to run Auto Config. This device can be either:
  - A delivery controller™
  - A domain joined machine with .NET Framework 4.7.2 or later and the Citrix PowerShell SDK. For Citrix PowerShell, you must install Citrix Studio.

BACK UP

1. Install Automated Configuration. For more information, see Download Automated Configuration.
2. Double-click **Auto-Config**.
3. On the PowerShell window, run the command `Backup-CvadAcToFile` to export all components. Exporting your on-premises configuration does not modify it.

After you run the command for the first time, the process creates a folder with the `.yml` configuration files at the following location: `%HOMEPATH%\Documents\Citrix\AutoConfig`.

The folder contains the backup files from the recent export, and each previous backup is stored in a subfolder.

RESTORE

1. Double-click **Auto-Config**.
2. Run the following command to do the restore:

```
Restore-CvadAcToSite -Environment OnPrem -RestoreFolder <folder path of the backup files>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. After you run the command, verify the state of the export, and the log folder is available at: `%HOMEPATH%\Documents\Citrix\AutoConfig`.
4. If there are any errors or exceptions, see the **Fixups** section in the log file.

DaaS

PREREQUISITES FOR BACKING UP YOUR CONFIGURATIONS

- A DaaS environment with an active resource location and Connector installed.
- Connectivity to sites accessing Citrix Cloud. For more information, see System and Connectivity Requirements.

NOTE

You cannot backup MCS from the cloud using Automated Configuration.

BACK UP

Backs up the following files:

- The `CustomerInfo.yml` file with your customer ID, client ID, and secret key information. For more information on the process to retrieve your customer ID, client ID, and secret key, see Generating the customer ID, client ID, and secret key. For information on how to add this information to the `CustomerInfo.yml` file, see Populating customer info file.
- The `ZoneMapping.yml` file with information that maps your resource locations in the cloud. For more information on how to map your zones, see the Populating zone mapping file.
- The `CvadAcSecurity.yml` file with information on host connections.

1. Install Automated Configuration. For more information, see Install Automated Configuration.

NOTE

For DaaS backups, install the Automated Configuration on a machine with Internet access and to which the administrator has direct access as well.

1. Double-click **Auto Config**.
2. On the PowerShell window, run the following command to take a backup: `Export-CvadAcToFile`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you run the command for the first time, the process creates a folder with the .yml configuration files at the following location: `%HOMEPATH%\Documents\Citrix\AutoConfig`

The folder contains the backup files from the recent export, and each previous backup is stored in a subfolder.

RESTORE

1. Double-click the **Auto Config**.
2. On the PowerShell window, run the following command to do the restore:

   ```
   Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
   ```

3. After you run the command, verify the state of the export, and you can locate the log folder at `%HOMEPATH%\Documents\Citrix\AutoConfig`.
4. If there are any errors or exceptions, see the **Fixups** section in the log file.

Granular migration

NOTE

For more information on the component migration order, see Component Migration Order.

RESTORE ENTIRE COMPONENTS

To restore a component, you must select one or more parameters.

For example, to restore the entire delivery group and machine catalog components, run the following command:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups
-MachineCatalogs
```

RESTORE COMPONENT MEMBERS

To restore one or more component members, use the `IncludeByName` feature. You must invoke the `Restore` cmdlet with the `Restorefolder` parameter along with the selected component, and the inclusion list.

For example, to restore two group policies from a backup:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -GroupPolicies
-IncludeByName Policy1,Policy2
```

RESTORE COMPLETE CLOUD SITE CONFIGURATION

To restore all the components or the entire cloud site, run the following command:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

Automated Configuration tool for backup and restore

The Automated Configuration tool commands trigger the backup and restore APIs that Studio uses.

The `BckRstr` cmdlets log to console. Folders with logging information are not created in `\Documents\Citrix\AutoConfig`.

NOTE:

The prerequisites for backing up your configurations in Citrix Virtual Apps and Desktops and Citrix DaaS™ is same as Automated Configuration tool in the PowerShell session.

Backup

For starting a new backup action on the Delivery Controller, run `New-BckRstrBackup` on the PowerShell window.

Restore

For restoring members from a single component from an existing backup, run `Restore-BckRstrBackups` on the PowerShell window.

For the complete list of commands, see Automated configuration tool cmdlets for backup and restore.

Best practices for backup and restore

This article provides several recommendations that can help in better planning of backup and restore.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	BEST PRACTICE
Scheduling backups	Set up a default backup schedule, which can run at a daily, weekly, or monthly frequency based on how frequently you expect your site configuration to change. Set this default schedule for a less active window, possibly weekends, or midnight. For information on scheduled backups. see Create scheduled backups.
	If you have multiple backup schedules defined that might run on the same day, then use the **Settings** tab on the **Backup and Restore** node to reset the limit to one backup per day.
Managing backups	Always pin golden copy backups so that they are retained when the 30 backup limit is reached. Right-click a backup to pin the selected backup.

FAQ

Can custom admins do backup and restore?

No. Backup and restore functionality is limited to administrators with full rights.

Can we backup selective components?

No. Currently, the on-demand and scheduled backups back up the entire site configuration. Components have several dependencies and pre-requisites. To ensure proper resolution of these dependencies, you can back up components in entirety. You can however, restore selective components.

Can we download backups?

Currently, use ACT to download backups from your DaaS site. You can download ACT from Automated Configuration for Virtual Apps and Desktops.

Can we backup and restore MCS catalogs?

Currently, we cannot backup and restore MCS catalogs. You can use ACT to back up your MCS catalogs and import them into another site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrate configuration to Citrix Cloud™

Automated Configuration Tool (ACT) allows migration of Citrix Virtual Apps and Desktops™ configuration (policies, applications, catalogs, admin roles, scopes, and others) from one or more on-premises sites to Citrix DaaS hosted on Citrix Cloud. It can also be used to migrate information between different Cloud regions or tenants.

This tool discovers and exports one or more on-premises sites as a collection of configuration files, which you can optionally edit. These files' configuration can then be imported into Citrix DaaS. The migration is done in stages by running the tool multiple times, allowing you to easily achieve the desired configuration state.

ACT isn't just a one and done migration tool. You can use it to manage your day-to-day cloud operations such as:

- Automating the transfer from test or stage cloud accounts to production cloud accounts
- Backing up and restoring your configuration
- Splitting one cloud environment into multiple clouds

The following *2-minute* video provides a quick tour of Automated Configuration.

<iframe src="https://www.youtube.com/embed/uyQ9o2L1DXQ" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
For additional information on Automated Configuration, see Proof of Concept: Automated Configuration Tool on Tech Zone.

For a deeper look into moving your deployment and readying your on-premises configuration for migration, see Deployment Guide: Migrating Citrix Virtual Apps and Desktops from on-premises to Citrix Cloud on Tech Zone.

Known limitations

- Machine catalogs provisioned through Machine Creation Services™ have special considerations. For more information on MCS, see Understand migrating Machine Creation Services provisioned catalogs.

Prerequisites for migrating your configuration

For *exporting* your configuration from Citrix Virtual Apps and Desktops, you need:

- Citrix Virtual Apps and Desktops: current release and its immediate predecessor or Citrix Virtual Apps and Desktops, XenApp and XenDesktop® LTSRs: all versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A domain-joined machine with .NET Framework 4.7.2 or later and the Citrix PowerShell SDK. This is automatically installed on the Delivery Controller. (To run on machine other than the on-premises Delivery Controller, Citrix Studio must be installed, as Studio installs the correct PowerShell snap-ins. The Studio installer can be found on the Citrix Virtual Apps and Desktops installation media.)

For *importing* your configuration into Citrix DaaS, you need:

- A machine with access to Citrix Cloud. This does not have to be a Delivery Controller™ or a domain-joined machine.
- Citrix DaaS provisioned.
- An active resource location with Connector installed and domain-joined to the same domain as the on-premises setup.
- Connectivity to sites accessing Citrix Cloud must be allowed and available. For more information, see System and Connectivity Requirements.

NOTE:

Automated Configuration cannot be installed on a Cloud Connector system.

Key steps

1. Download the Automated Configuration Tool and review the system requirements. See Download Automated Configuration.
2. Populate the `CustomerInfo.yml` file with your `CustomerName`, `CustomerID`, and `SecretKey` values generated from the Citrix Cloud portal. See Generate the customer ID, client ID, and secret key and Populate the customer info file.
3. If the on-premises site contains multiple zones, update the `ZoneMapping.yml` file to map zones to Citrix DaaS resource locations. See Populate zone mapping file.
4. If the site contains multiple hosting connections, update the `CvadAcSecurity.yml` file with the connection information for each host type migrating into Citrix DaaS. If only a single host connection, update the `CvadACSecurity.yml` file with the connection information for the host connection. See Update the security file for host connections.
5. Open ACT and export your on-premises site using the `Export-CvadAcToFile` command. See Supported migration objects for the list of components supported for migration. For information on the steps to export, see Export on-premises configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Import components in stages using the `Merge-CvadAcToSite` command. Alternatively, migrate the entire site at once. Ensure you migrate components in the order listed in Component migration order. For information on the steps to import, see Run an import.
7. Activate the cloud site. See Activate sites.

Download Automated Configuration

Download and install the Automated Configuration tool from Citrix Downloads.

Upgrade Automated Configuration

To prevent errors in functionality, always use the latest available version of ACT.

To know about your tool version, do the following:

1. Double-click the **Auto Config** icon. A PowerShell window appears.
2. Run the following command to check your version number.

```
Get-CvadAcStatus
```

3. Check your tool version against the version listed in Citrix Downloads. The latest version of the tool is located there.
4. Download and install the latest version of the tool. You do *not* need to uninstall the old version to upgrade Automated Configuration.

NOTE:

When you run cmdlets to access the cloud in Automated Configuration, the tool alerts you when there is a newer version available for download. For more information on cmdlets, see Automated Configuration tool cmdlets.

Generate the customer ID, client ID, and secret key

To migrate the on-premises site to Citrix DaaS, populate the `CustomerInfo.yml` file with the customer ID, client ID, and secret key from Citrix Cloud portal.

To retrieve the Customer ID:

1. Sign into your Citrix Cloud account and select the customer.
2. Click the grid icon and select **Identity and Access Management**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Navigate to **API access > Secure clients**. The customer Id is displayed on the page.

To retrieve the Client ID and Secret Key:

1. On the **Secure clients** page, enter a name in the box. This name is used to differentiate between multiple client IDs and secret keys.
2. Click Create Client to create the client ID and the secret key.
3. Copy the client ID and secret key to a secure location and download the `.csv` file containing this information. Use the `.csv` file to populate the `CustomerInfo.yml` file.

NOTE:

- The client ID and secret key do not expire. If they are compromised, immediately remove them by using the **Trash** icon and create new ones.
- The secret key cannot be retrieved if it is lost or forgotten; a new client ID and secret key must be created.

Populate customer info file

The `CustomerInfo.yml` file eliminates the need to provide customer information parameters every time while running the cmdlet. Any of the customer information can be overridden by using cmdlet parameters.

Use `New-CvadAcCustomerInfoFile` cmdlet to create the `CustomerInfo.yml` file.

IMPORTANT:

Do not manually edit the `CustomerInfo.yml` file. Doing so can cause inadvertent formatting errors.

The `New-CvadAcCustomerInfoFile` cmdlet has the following required parameters.

- CustomerId – customer's ID.
- ClientId – customer's client ID created on Citrix Cloud.
- Secret – customer's secret created on Citrix Cloud.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId
6813EEA6-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaaw==
```

You can also create the `CustomerInfo.yml` using the `SecurityCsvFileSpec` parameter that points to the downloaded `security.csv` file. You must also specify the CustomerId.

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:
\Users\my_user_name\downloads/security.csv -CustomerId markhof123
```

Use `Set-CvadAcCustomerInfoFile` cmdlet to update the `CustomerInfo.yml` file. This cmdlet only changes the Client ID.

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

The following is a sample CustomerInfo.yml file.

```
# Created/Updated on 2020/01/29 16:46:47

CustomerId: ‘markhof123’

ClientId: ‘6713FEA6-46CC-4F8A-BC71-539F2DDK5384’

Secret: ‘TwBLaaabbbaaaaaaaaaaw==’

Environment: Production

AltRootUrl: ‘’

StopOnError: False

AlternateFolder: ‘’

Locale: ‘en-us’

Editor: ‘C:\Program Files\Notepad++\notepad++.exe’

Confirm: True

DisplayLog: True
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Populate zone mapping file

An on-premises zone is the equivalent of the cloud resource location. Unlike other site components, you cannot import the on-premises zone to the cloud automatically. Instead, it must be manually mapped using the `ZoneMapping.yml` file. Import failures can occur if the zone name is not associated with an existing resource location name.

If the on-premises sites have only one zone and cloud sites have only one resource location, the Automated Configuration tool makes the correct association, eliminating the need to manually manage the `ZoneMapping.yml` file.

However, if the on-premises sites have multiple zones or cloud sites have multiple resource locations, then manually update the `ZoneMapping.yml` file to reflect the correct mapping of on-premises zones to cloud resource locations.

The `ZoneMapping.yml` file is located in `%HOMEPATH%\Documents\Citrix\AutoConfig`. The content of the `.yml` file is a dictionary with the zone name as the key and the resource location name as the value.

For example, an on-premises Citrix Virtual Apps and Desktops site with a primary zone called "Zone-1" and a secondary zone called "Zone-2" is migrated to a Citrix DaaS deployment with two newly created cloud resource locations called "Cloud-RL-1" and "Cloud-RL-2". In this instance, the ZoneMapping.yml would be configured as follows:

```
            Zone-1: Cloud-RL-1



            Zone-2: Cloud-RL-2
```

NOTE:

Add a space between the colon and resource location name. If spaces are used in the zone or resource location name, enclose the name with quotes.

Update the security file for host connections

Host connections and their associated hypervisors can be exported and imported using ACT.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Adding a hypervisor to a host connection requires security information specific to the type of hypervisor. This information cannot be exported from the on-premises site for security considerations. You must manually provide the information so that Automated Configuration can successfully import host connections and hypervisors to the cloud site.

The export process creates the `CvadAcSecurity.yml` file in `%HOMEPATH%\Documents\Citrix\AutoConfig` containing placeholders for each security item needed for the specific hypervisor type. You must update the `CvadAcSecurity.yml` file before importing into the cloud site. Administrator updates are retained over multiple exports with new security placeholders added as needed. Security items are never removed. For more information, see Manually update the CvadAcSecurity.yml file

```
HostConn1:

ConnectionType: XenServer®

UserName: root

PasswordKey: rootPassword

HostCon2:

ConnectionType: AWS

ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH

SecretKey: TwBLaaaaaaaaaaaaaaaaw==

Region: East
```

Per-hypervisor security information

The following lists the security information required for each hypervisor type.

- XenServer, Hyper-V, VMware
  - User Name
  - Clear-text Password
- Microsoft Azure
  - Subscription ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Application ID
    - Application Secret
- AWS
    - Service Account ID
    - Application Secret
    - Region

Special security considerations

All security information is entered as clear text. If clear text is not recommended, the host connections and associated hypervisors can be manually created using **Studio**. The host connections and hypervisor names must match their on-premises counterparts exactly so that machine catalogs that use the host connections can be successfully imported.

Export your Citrix Virtual Apps and Desktops on-premises configuration

Using an `export` PowerShell command, you can export your existing on-premises configuration and obtain the necessary `.yml` files. These files are used to import your desired configuration into Citrix Cloud.

Supported migration objects

Automated Configuration supports moving the configuration of the following components:

- Tags
- Delegated Admin
    - Scopes
    - Roles
- Host Connections
    - A Single Resource Pool
    - Admin Scopes
- Machine Catalogs
    - Admin Scopes
    - Machines

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Remote PC Access, Physical, Pooled, Provisioned, MCS, Assigned
- StoreFront™
- Delivery Groups
    - Access Policy
    - Admin Scope Association
    - Application Access Policy
    - Assignment Policy
    - Entitlement/Desktop Policy
    - Power Schedules
    - Session Lingering
    - Session Prelaunch
    - Reboot Schedules
    - Tags
- Application Groups
    - Admin Scope Association
    - Delivery Groups
    - Users and Groups
- Applications
    - Application Folders
    - Icons
    - Applications
    - Broker Configured FTAs
    - Tags
- Group Policies
- User Zone Preferences

Export on-premises configuration

1. Double-click the **Auto Config** icon. A PowerShell window appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Run the following command to export all components. Exporting your on-premises configuration does *not* change it in any way.

```
Export-CvadAcToFile
```

After you run any cmdlet for the first time, an export folder with the `.yml` configuration files and logs is created. The folder is at `%HOMEPATH%\Documents\Citrix\AutoConfig`. Each successive export creates a subfolder. The parent folder `%HOMEPATH%\Documents\Citrix\AutoConfig` always contains the exported files from the most recent export.

NOTE:

If Automated Configuration is not installed on the Delivery Controller, run `import-module Citrix.AutoConfig.Commands` before using the tool through PowerShell. This step is not needed if you open Automated Configuration using the **Auto Config** icon.

If you encounter any errors or exceptions, see the **Fixups** section in the log file.

Import your configuration to Citrix DaaS

IMPORTANT:

- When migrating an on-premises deployment to cloud, make sure that the domain and OU GPOs that contain the Citrix settings are migrated to cloud. Citrix Web Studio™ does not support GPMC and hence, the domain and OU GPOs are not visible in the Web Studio. The Citrix policy engine enforces the domain and OU GPOs on VDAs and users that are in the domains and OUs. Post log in to a VDA, a user might see that the policies from the domain and OU GPOs are applied to their session. However, administrators cannot see these policies and settings which might lead to confusions.

Component migration order

The components and their dependencies are listed here. A component's dependencies must be in place before it can be imported or merged. If a dependency is missing, it can cause the import or merge command to fail. The **Fixups** section of the log file shows missing dependencies if an import or merge fails.

1. Tags

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- No pre-dependencies

2. Delegated Admin
    - No pre-dependencies
3. Host Connections
    - Security Information in CvadAcSecurity.yml
4. Machine Catalogs
    - Machines present in Active Directory
    - Host Connections
    - Tags
5. StoreFront
6. Delivery Groups
    - Machines present in Active Directory
    - Users present in Active Directory
    - Machine Catalogs
    - Tags
7. Application Groups
    - Delivery Groups
    - Tags
8. Applications
    - Delivery Groups
    - Application Groups
    - Tags
9. Group Policies
    - Delivery Groups
    - Tags
10. User Zone Preferences

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Run an import

1. Double-click the **Auto Config** icon. A PowerShell window appears.
2. Run the following command to import all components.

```
Merge-CvadAcToSite
```

Verify the expected state with the new current state. Various import options control whether the import results are identical or a subset of the on-premises site.

After you run the cmdlet, an export folder with the `.yml` configuration files and logs is created. The folder is at `%HOMEPATH%\Documents\Citrix\AutoConfig`.

If you encounter any errors or exceptions, see the **Fixups** section in the log file.

NOTE:

If Automated Configuration is not installed on the Delivery Controller, run `import-module Citrix.AutoConfig.Commands` before using the tool through PowerShell. This step is not needed if you open Automated Configuration using the **Auto Config** icon.

To revert to your original Citrix DaaS configuration, see Backing up your Citrix DaaS configuration.

Understand import operation

The import process is designed to accurately perform updates, only perform needed updates and verify that all updates have been correctly made. The steps are followed in all import operations:

1. Read the exported .yml file (expected state).
2. Read the cloud (current state).
3. Back up the pre-import cloud state to .yml files (pre-backup can be restored if necessary).
4. Evaluate the differences between the expected and current state. This determines which updates to make.
5. Make the updates.
6. Reread the cloud (new current state).
7. Back up the post-import cloud state to .yml files (post-backup can be restored if necessary).
8. Compare the new current state with the expected state.
9. Report the results of the comparison.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Granular migration

IMPORTANT:

For more information on component migration order, see Component migration order.

You can selectively migrate components only or even component names only.

- Component parameters supported include `MachineCatalogs`, `Tags`, and more.
- Component name parameters supported include `IncludeByName` and `ExcludeByName` parameters, and others.

For more information on parameters and how to use them, see Granular migration parameters.

Activate sites

The delivery controller in both on-premises and cloud sites controls resources such as brokering desktops, applications, and rebooting machines. Problems occur when a common set of resources is controlled by two or more sites. Such a situation can occur when migrating from an on-premises site to a cloud site. It is possible for both the on-premises and cloud delivery controllers to manage the same set of resources. Such dual management can lead to resources becoming unavailable and unmanageable, and can be difficult to diagnose.

Site activation allows you to control where the active site is controlled.

Site activation is managed using the delivery group maintenance mode. Delivery groups are placed in maintenance mode when the site is inactive. Maintenance mode is removed from delivery groups for sites that are active.

Site activation does not affect or manage VDA registration or machine catalogs.

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

All cmdlets support the `IncludeByName` and `ExcludeByName` filtering. This parameter allows you to select which delivery groups can have their maintenance mode changed. Delivery groups can be selectively changed as needed.

Import and transferring control to the cloud

The following is a high-level description on how to import and transfer control from the on-prem site to the cloud site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Export and import the on-premises site to the cloud. Make sure the `–SiteActive` parameter is not present on any of the import cmdlets. The on-premises site is active and the cloud site inactive. By default, cloud site delivery groups are in maintenance mode.
2. Verify the cloud content and configuration.
3. During off hours, set the on-premises site to inactive. The `–SiteActive` parameter must be absent. All on-premises site delivery groups are in maintenance mode.
    - `Set-CvadAcSiteActiveStateOnPrem`
4. Set the cloud site to active. The `–SiteActive` parameter must be present. No cloud site delivery groups are in maintenance mode.
    - `Set-CvadAcSiteActiveStateCloud –SiteActive`
5. Verify that the cloud site is active and the on-premises site is inactive.

Transfer control back to the on-premises site

To transfer control from the cloud site to the on-premises site:

1. During off hours, set the cloud site to inactive. All cloud site delivery groups are in maintenance mode.
    - `Set-CvadAcSiteActiveStateCloud`
2. Set the on-premises site to active. No on-prem site delivery groups are in maintenance mode.
    - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

Additional site activation information

- If no machines are power managed and there are no reboot schedules (which usually means there are no host connections either) all cloud delivery groups can be imported as active. Add `-SiteActive` to `Merge-CvadAcToSite` / `Import-CvadAcToSite` or run `Set-CvadAcSiteActiveStateCloud -SiteActive` after importing.
- If machines are power managed or there are reboot schedules, a different process is needed. For example, when switching from on-premises to cloud in this situation, set the on-premises site to inactive using `Set-CvadAcSiteActiveStateOnPrem`. Then, set the cloud site to active using `Set-CvadAcSiteActiveStateCloud -SiteActive`.
- The `Set-CvadAcSiteActiveStateCloud` and `Set-CvadAcSiteActiveStateOnPrem` cmdlets are also used to reverse the process. For example, run `Set-`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`CvadAcSiteActiveStateCloud` without the `-SiteActive` parameter, then run `Set-CvadAcSiteActiveStateOnPrem` with the `-SiteActive` parameter.

Understand migrating Machine Creation Services provisioned catalogs

NOTE:

This feature is available only on versions 3.0 and later. Check your version by using `Get-CvadAcStatus` within Automated Configuration.

Machine Creation Services (MCS) catalogs create two different types of catalogs:

- When changes made to a machine are lost or reversed (Commonly Server OS, where applications are published) – this is a pooled VDI / multi-session use case
- When changes made to a machine are preserved across reboot (Commonly client OS with a dedicated user) – this is a static VDI use case

The type of catalog can be confirmed in the catalog node in Citrix Studio and looking at the "User data:" value of the catalog.

NOTE:

MCS cannot be backed up from the cloud using Automated Configuration.

Pooled VDI / multi-session catalogs

Catalogs with "User data: Discard" are pooled VDI catalogs and can only migrate the main image and configuration. Any virtual machines in these catalogs are not migrated. This is because the life cycle of the virtual machine is maintained by the site you are importing from, which means every time the machines are turned on, its state might change. This makes import impossible as the import data for the virtual machines quickly gets of out of sync.

When you are migrating these catalogs using the tool, it creates catalog metadata and initiates main image creation, but no machines are imported.

Since this process can take some time to be created based on the size of the main image, the import command within the tool only starts the MCS catalog creation and does not wait for it to finish. After the import has completed, monitor the catalog creation progress using Studio in the cloud deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Once the main image is created, you can provision machines. Consider the capacity considerations because you would have capacity consumed from your on-premises usage.

All other objects (delivery groups, applications, policies, and so forth) that use that catalog can be imported and do not have to wait for the main image creation. When the catalog has finished creating, machines can be added to the imported catalog and then users can launch their resources.

NOTE:

Use the same commands available within the tool to migrate catalogs and all other objects.

Static VDI catalogs

NOTE:

Since this operation imports low-level details that are stored in the database, this process must be run from a machine with database access.

The static VDI catalogs migrate the main image, configurations, and all virtual machines. Unlike the pooled VDI use case, no images need to be created.

The VDAs must be pointed to the connector for them to register with the cloud.

Refer to the Activating sites section to make the cloud site active, so that the reboot schedule, power management, and other items are controlled by the cloud.

Once the migration is completed, if you want to delete this catalog from your on-premises site, you must select **leave VM and AD account**. Otherwise, they are deleted and the cloud site would be left pointing to the deleted VM.

Update MCS tags to detect orphaned resources after migration

After you migrate from on-premises configuration to a cloud site, or from your cloud configuration to another cloud site, you must update the MCS site id tags in case of persistent VMs so that orphaned resources can be detected correctly. To do this, use the PowerShell command `Set-ProvResourceTags`. Currently, this feature is applicable to Azure.

The detailed steps are as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Update the MCS site id tags from the new Citrix site using the PowerShell command `Set-ProvResourceTags`. For example:

   ```
   Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

   Or,

   ```
   Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

The parameter details are as follows:

- `ProvisioningSchemeUid` or `ProvisioningSchemeName` is a mandatory parameter.
- `VMName` is an optional parameter. If no `VMName` is specified, tags of all the VMs of this machine catalog are updated.
- `VMBatchSize` is an optional parameter to divide all VMs into batches. If no `VMBatchSize` is specified, the default value (10) is applied. The range is from 1 through 60.
- `ResourceType` can be one of the following:
  - `MachineCatalog`: For updating tags of machine catalog resources.
  - `VirtualMachine`: For updating tags of VM related resources.
  - `All`: (default ResourceType): For updating tags of both machine catalog and VM related resources.

Merge multiple sites into a single site

Multi-site support for Automated Configuration provides a method to merge multiple on-premises sites into a single cloud site.

Multi-site support adds unique prefixes and suffixes to component names on a per on-premises-site basis, ensuring name uniqueness after multiple on-premises sites are merged to a single cloud site.

Prefixes and suffixes can be assigned for each of the following components on a per-on-premises-site basis.

- `AdminScope`
- `AdminRole`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront`
- `Tag`

Application folders support prefixing, suffixing, and rerooting. Rerooting adds an extra top-level folder to an application's existing folder structure.

Prefix and suffix rules

1. Prefixes and suffixes cannot contain any of the following special characters: `\ , / ; : # . * ? = < > | ( ) " ' { } [ ]`
2. Prefixes and suffixes can contain trailing spaces but not leading spaces.
3. Prefixes and suffixes must be double quoted to contain trailing spaces.
4. Prefixes and suffixes are applied at the time of import, merge, and add. The source `.yml` files are never modified.
5. The prefix and suffix process automatically prefixes or suffixes dependent component names when applicable. For example, if machine catalog names are prefixed with "East," then the delivery groups referencing them are also prefixed with "East."
6. If a component name already begins with the prefix or suffix, no prefix or suffix is added. Component names cannot contain double identical prefixes or suffixes.
7. Prefixes and suffixes can be individually used or used in combination.
8. Use of a prefix or a suffix on a component is optional.

NOTE:

The Studio displays components in alphabetical order.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Group components by site

Use prefixing to visually group components from a single site. Each site is listed in its own group with prefixing alphabetically controlling the ordering of different site groups.

Group components by name

Use suffixing to visually group like-named components from multiple sites. Like-named components from different sites visually alternate.

Prefix and suffix mapping file

Site prefixing begins with the `SiteMerging.yml` file that contains the site prefix and suffix mapping for one or more on-premises sites. You can manage the `SiteMerging.yml` file manually, or by using the available cmdlets listed at the Merging multiple on-premises sites cmdlets section.

Export on-premises site

Merging cannot begin until you have exported an on-premises site. To export an on-premises site, see Export on-premises configuration.

Central export target folder

The methods described in this section place multiple site exports into a central file share location. The `SiteMerging.yml` file, `CustomerInfo.yml` file, and all export files reside in that file share location, allowing you to do the import from one location independent of the on-premises sites.

Cloud-accessing operations never reference the on-premises sites or Active Directory, therefore allowing you to do cloud-accessing operations from anywhere.

There are two methods to do this:

- Direct file share: To import, merge, or add from the direct file share, you must decide from which machine you want to do the cloud accessing operation
- File share reference using `SiteMerging.yml`: This method uses the `SiteRootFolder` member of the site's prefixes set and reduces the odds of targeting the wrong folder when exporting, importing, merging, or adding.

If you do not use a central file share method, then do the import, merge, or add from the individual Delivery Controllers. Create and replicate the `SiteMerging.yml` file on each Delivery Controller being migrated into the cloud. The default location is `%HOMEPATH%\Documents\Citrix\AutoConfig`. You must specify the `-SiteName` parameter to select the correct site prefixes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Direct file share

The export, import, merge, and new/add operations provide a parameter to target or source a folder other than the default folder, *%HOMEPATH%\Documents\Citrix\AutoConfig*. The following examples use a central file share at `\\share.central.net` that the admin already has access to, having provided credentials as needed.

To target the export to a site-specific folder, use the `–TargetFolder` parameter:

From the East Delivery Controller™:

```
mkdir  \\share.central.net\AutoConfig\SiteEast



Export-CvadAcToFile   –TargetFolder   \
\share.central.net\AutoConfig\SiteEast
```

From the West Delivery Controller:

```
mkdir  \\share.central.net\AutoConfig\SiteWest



Export-CvadAcToFile   –TargetFolder   \
\share.central.net\AutoConfig\SiteWest`
```

After the exports are complete, create the CustomerInfo.yml and SiteMerging.yml files and place them in `\\share.central.net\AutoConfig`.

NOTE:

Do not use the `SiteRootFolder` parameter when creating the SitePrefixes.yml when using this direct file share reference method.

To import, merge, or add from the direct file share, you must decide from which machine you want to do the cloud accessing operation. Options include:

- One of the on-premises Delivery Controllers where the tool is already installed.
- The machine hosting the file share.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A different machine.

Automated Configuration must be installed on the machine accessing the cloud. Neither the on-premises PowerShell SDK, Delivery Controller, nor Active Directory are used, so the cloud accessing execution requirements are simpler than the export requirements.

To merge the East Delivery Controller to the cloud:

```
Merge-CvadAcToSite –SiteName East –SourceFolder  \
\share.central.net\AutoConfig\SiteEast -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

To merge the West Delivery Controller to the cloud:

```
Merge-CvadAcToSite –SiteName West –SourceFolder  \
\share.central.net\AutoConfig\SiteWest -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

The following is a sample `SitePrefixes.yml` file used in the previous example.

```
East:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    HostConnectionPrefix: "East_"
    MachineCatalogPrefix: "East_"
    StoreFrontPrefix: "East_"
    TagPrefix: "East_"
    AdminScopeSuffix: "_east"
    AdminRoleSuffix: "_east"
    ApplicationAdminSuffix: "_east"
    ApplicationFolderSuffix: "_east"
    ApplicationGroupSuffix: "_east"
    ApplicationUserSuffix: "_east"
    DeliveryGroupSuffix: "_east"
    GroupPolicySuffix: "_east"
    HostConnectionSuffix: "_east"
    MachineCatalogSuffix: "_east"
    StoreFrontSuffix: "_east"
    TagSuffix: "_east"
  West:
    SiteRootFolder: "" # Important: leave this empty
    AdminScopePrefix: "Western "
    AdminRolePrefix: "Western "
    ApplicationAdminPrefix: "Western "
    ApplicationFolderPrefix: "" # Note that a new parent root folder is used
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "

  AdminScopeSuffix: ""

  AdminRoleSuffix: ""

  ApplicationAdminSuffix: ""

  ApplicationFolderSuffix: ""

  ApplicationGroupSuffix: ""

  ApplicationUserSuffix: ""

  DeliveryGroupSuffix: ""

  GroupPolicySuffix: ""

  HostConnectionSuffix: ""

  MachineCatalogSuffix: ""

  StoreFrontSuffix: ""
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  TagSuffix: ""
```

File share reference using SiteMerging.yml

This method uses the `SiteRootFolder` member of the site's prefixes set. While more involved than the direct file share method, this method reduces the odds of targeting the wrong folder when exporting, importing, merging, or adding.

First, set the `SiteRootFolder` for each site in the SiteMerging.yml file. You must do this on the shared location.

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \
\share.central.net\AutoConfig\SiteEast -SitePrefixesFolder  \
\share.central.net\AutoConfig



New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest
-SitePrefixesFolder  \\share.central.net\AutoConfig
```

In this example, East is a fully qualified folder specification and West is a relative folder specification.

To target the export to a site-specific folder using the SiteMerging.yml file:

From the East Delivery Controller:

```
mkdir  \\share.central.net\AutoConfig\SiteEast



Export-CvadAcToFile   -SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

From the West Delivery Controller:

```
mkdir  \\share.central.net\AutoConfig\SiteWest
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Export-CvadAcToFile   -SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

The export cmdlet uses the CustomerInfo.yml folder location to locate the SiteMerging.yml file. In the case of East, the `SiteRootFolder` is fully qualified. It is used as-is. In the case of West, the `SiteRootFolder` is not fully qualified. It is combined with the CustomerInfo.yml folder location to retrieve a fully qualified folder location for West.

To merge the East Delivery Controller to the cloud:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

To merge the West Delivery Controller to the cloud:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

The following is a sample SitePrefixes.yml file used in the previous example.

```
  East:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    GroupPolicyPrefix: "East_"
    HostConnectionPrefix: "East_"
    MachineCatalogPrefix: "East_"
    StoreFrontPrefix: "East_"
    TagPrefix: "East_"
    AdminScopeSuffix: "_east"
    AdminRoleSuffix: "_east"
    ApplicationAdminSuffix: "_east"
    ApplicationFolderSuffix: "_east"
    ApplicationGroupSuffix: "_east"
    ApplicationUserSuffix: "_east"
    DeliveryGroupSuffix: "_east"
    GroupPolicySuffix: "_east"
    HostConnectionSuffix: "_east"
    MachineCatalogSuffix: "_east"
    StoreFrontSuffix: "_east"
    TagSuffix: "_east"
  West:
    SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"
    AdminScopePrefix: "Western "
    AdminRolePrefix: "Western "
    ApplicationAdminPrefix: "Western "
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "

  AdminScopeSuffix: ""

  AdminRoleSuffix: ""

  ApplicationAdminSuffix: ""

  ApplicationFolderSuffix: ""

  ApplicationGroupSuffix: ""

  ApplicationUserSuffix: ""

  DeliveryGroupSuffix: ""

  GroupPolicySuffix: ""

  HostConnectionSuffix: ""

  MachineCatalogSuffix: ""

  StoreFrontSuffix: ""
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
TagSuffix: ""
```

Merge the sites

Citrix® recommends performing the cloud operations in steps and to do a complete review of each result before doing the next cloud operation. For example, if merging three sites to a single cloud site:

1. Merge the initial site to the cloud using the appropriate `SiteName` value.
2. Review the results in Studio.
3. If the results are incorrect, determine the issue and its cause, correct it, and then rerun the merge. If necessary, remove the cloud components and start from scratch by using `Remove-CvadAcFromSite` for the selected component and members. If the results are correct, continue.
4. If the initial merge is correct, merge the second site to the single cloud site.
5. Repeat steps 2 and 3.
6. If the second merge is correct, merge the third site to the single cloud site.
7. Repeat steps 2 and 3.
8. Review the resources from the user's perspective and verify that the view is in the desired state.

Remove a component using the site prefix

You can selectively remove single site components by using the prefix on the `–IncludeByName` parameter of the `Remove-CvadAcFromSite` cmdlet. In the following example, the West Delivery Controller delivery groups are not correct. To remove the delivery groups for just the West site:

```
Remove-CvadAcFromSite   –DeliveryGroups   –IncludeByName “Western *”
```

To remove all West components, run the following cmdlets in order.

`Remove-CvadAcFromSite –GroupPolicies –IncludeByName “Western *”`

`Remove-CvadAcFromSite –Applications –IncludeByName “Western *”`

`Remove-CvadAcFromSite – ApplicationGroups –IncludeByName “Western *”`

`Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Remove-CvadAcFromSite –MachineCatalogs –IncludeByName “Western *”
```

```
Remove-CvadAcFromSite –HostConnections –IncludeByName “Western *”
```

```
Remove-CvadAcFromSite –Tags –IncludeByName “Western *”
```

To remove group policies of the East components, use the suffix:

```
Remove-CvadAcFromSite   –GroupPolicies   –IncludeByName “*_east”
```

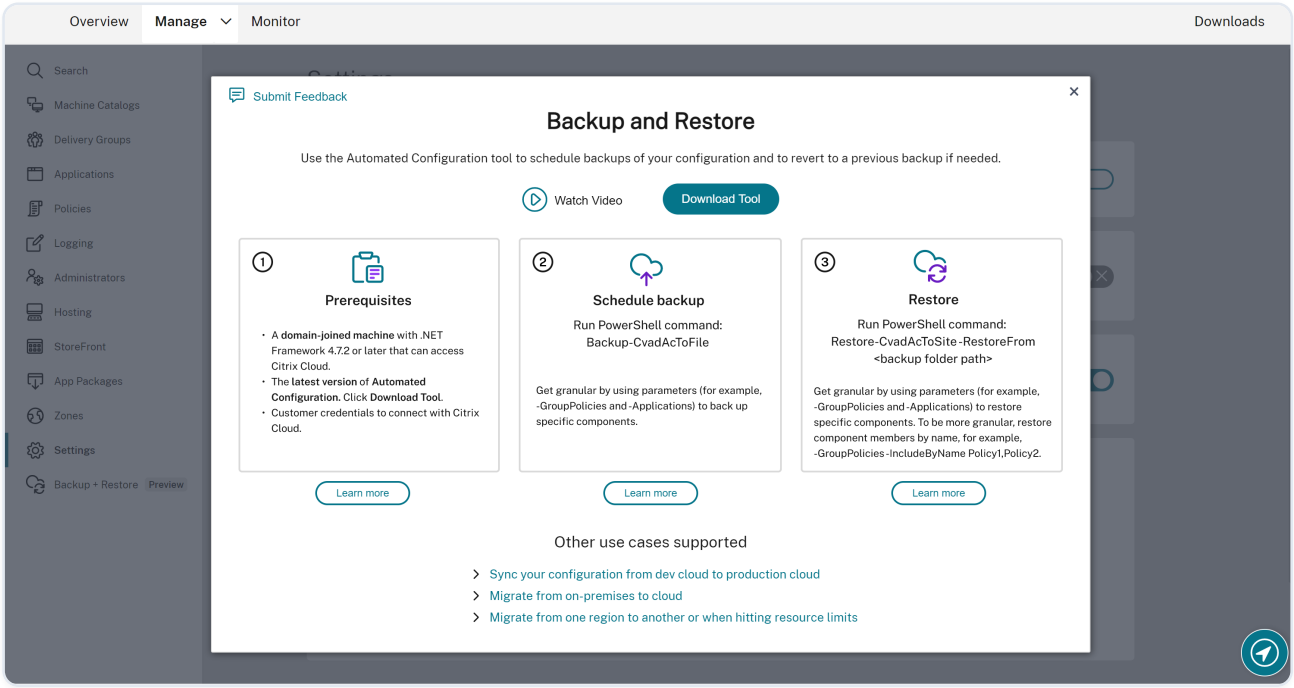
Migrate from cloud to cloud

Automated Configuration allows you to automate moving your cloud configuration to another cloud site or allowing you to restore your own cloud site.

Using Automated Configuration can solve many use cases:

- Syncing your site from test or stage to production
- Backing up and restoring your configuration
- Reaching resource limits
- Migrating from one region to another

In Studio on Citrix Cloud™, see the Backup and Restore node for information about Automated Configuration and how it can be used to migrate your configuration from cloud to cloud.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites for migrating your configuration

For backing up and restoring your configuration, you need:

- Citrix DaaS™ provisioned.
- An active resource location with Connector installed.
- Connectivity to sites accessing Citrix Cloud must be allowed and available. For more information, see System and Connectivity Requirements.

NOTE:

MCS cannot be backed up from the cloud using Automated Configuration.

Back up your Citrix DaaS configuration

Requirements

Do the following before backing up your Citrix DaaS configuration:

1. Populate the `CustomerInfo.yml` file with your customer ID, client ID, and the secret key information included. For more information on how to retrieve your customer ID, client ID and secret key, see Generate the customer ID, client ID, and secret key. For information on how to add this information to the `CustomerInfo.yml` file, see Populate customer info file.

When you run the backup commands, the `CustomerInfo.yml` must have the details of the source site customer from where you are taking the backup.

When you run the restore commands, the `CustomerInfo.yml` must have the details of the destination site customer to where you are restoring the configurations.

1. Populate the `ZoneMapping.yml` file with information that maps your resource locations in the cloud. For more information on how to map your zones, see Populate zone mapping file.
2. If you have host connections, you must input the corresponding information in the `CvadAcSecurity.yml` file. See Update the security file for host connections

Steps to back up your Citrix DaaS configuration

1. Install Automated Configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> For cloud-to-cloud migration, Automated Configuration can be installed on a machine having access to the internet that the administrator has direct access to.

2. Double-click the **Auto Config** icon. A PowerShell window appears.
3. Run the following command to do a backup.

```
Backup-CvadAcToFile
```

After you run any cmdlet for the first time, an export folder with the `.yml` configuration files and logs is created. The folder is at `%HOMEPATH%\Documents\Citrix\AutoConfig`.

If you encounter any errors or exceptions, see the **Fixups** section in the log file.

Restore your configuration to Citrix DaaS

1. Double-click the **Auto Config** icon. A PowerShell window appears.
2. Run the following command to do a restore.

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

Verify the expected state with the new current state.

After you run the cmdlet, an export folder with the `.yml` configuration files and logs is created. The folder is at *%HOMEPATH%\Documents\Citrix\AutoConfig*.

If you encounter any errors or exceptions, see the **Fixups** section in the log file.

The backup and restore process protects you from unintentional cloud site configuration changes or corruption. While Automated Configuration makes backups each time a change is made, this backup reflects the state of the cloud site configuration before the changes. Protecting yourself requires that you periodically back up your cloud site configuration and saving it in a safe place. If an undesirable change or corruption takes place, the backup can be used to fix the change or corruption at either a granular or full site configuration level.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Granular migration

IMPORTANT:

For more information on component migration orders, see Component migration order.

Restore all components

Restoring one component involves selecting one or more component parameters.

To restore the:

- entire delivery group and machine catalog components
- full cloud site configuration

follow this example:

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

Restore component members

Restoring one or more component members uses the `IncludeByName` feature. The `Restore` cmdlet is invoked with the `RestoreFolder` parameter along with the selected single component and the inclusion list.

To restore two group policies from a backup, follow this example:

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

```
-GroupPolicies -IncludeByName   Policy1,Policy2
```

```
-DeliveryGroups -MachineCatalogs`
```

Activate sites

Site activation allows you to control which site is active and controls your resources. For more information, see Activate sites.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrate Cloud configurations to on-premises

This article describes backing up and migrating your Cloud configurations to on-premises sites.

Pre-requisites for migrating your configuration

- Citrix Virtual Apps and Desktops™ on-premises environment with at least one registered VDA.
- Citrix Virtual Apps and Desktops on-premises environment running on one of the following versions:
  - The most recent Long-Term Service Release (LTSR) version - 2402.
  - Any of the Current Releases (CR) versions - 2308, 2311.
- Run the Automated Configuration tool (ACT) commands on a domain-joined machine with .Net 4.7.2 version or higher.
- A machine with the Citrix PowerShell SDK. PowerShell SDK is available within the Citrix Delivery Controller™ installable.

NOTE:

- If you are running the ACT on a different machine, it must be domain-joined and Studio must have the correct PowerShell snap-ins installed. To get the installer, go to Citrix Virtual Apps and Desktopsdownloads website.
- In the on-prem site, we recommend ACT be installed on the DDC. ACT can be started via the desktop icon.
- If ACT is intended to be used from the standard Powershell window, then run the following command: `Import-Module Citrix.AutoConfig.Commands`

ACT is not part of the system PowerShell path so must be explicitly imported.

Key steps

Follow the instructions to complete the migration of your Cloud configurations to on-premises:

1. Backup Cloud configuration.
2. Modify YML files.
3. Import configurations to on-premises.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Backup Cloud configuration

1. Install the **Automated Configuration**.
2. Double-click the **Auto Config** icon. A PowerShell window appears.
3. Run `New-CvadAcCustomerInfoFile` to create a **CustomerInfo.yml** file. For more information, see Populate customer info file.
4. Run the command `Backup-CvadAcToFile` to take a backup of your Cloud configurations.

NOTE:

- After you run any cmdlet for the first time, an backup folder with the .yml configuration files and logs is created. The folder is at `%HOMEPATH%\Documents\Citrix\AutoConfig`.
- If you encounter any errors or exceptions, see the **Fixups** section in the log file.
- Backup-CvadToFile does not support the parameters `IncludeByName` or `ExcludeByName`.

IMPORTANT:

Citrix recommends backing up all the components together.

Modify YML files

Modify the `.yml` files located at `%HOMEPATH%\Documents\Citrix\AutoConfig` to include the on-premises details as described in the following table:

YML FILE	PARAMETER	DESCRIPTION	EXAMPLES
CustomerInfo.yml	Environment	Change Environment to OnPrem. The environment parameter value is case-sensitive.	
ZoneMapping.yml	DaaS:CVAD	Map your Cloud resource locations to your on-premises zones.	It has to be old:new zones

© 1997–2026 Citrix Systems, Inc. All rights reserved.

YML FILE	PARAMETER	DESCRIPTION	EXAMPLES
CvadAcSecurity.yml	Hypervisor: ConnectionType: ‘ ‘ Username: ‘ ’ Password: ‘ ‘	Add the hypervisor username and passwords.	If the hypervisor is XenServer,XenServer: ConnectionType: ‘XenServer’ Username: ‘root’ Password: ‘ ‘

Import configurations to on-premises

1. Run either of the following commands in your on-premises site based on your requirements:
    a. `Merge-CvadAcToSite` - if there is an on-premises site running and you want to merge the Cloud configurations to it.
    b. `Import-CvadAcToSite -Environment OnPrem` - If on-premises configurations are not available and you are importing the Cloud configurations to create one.

IMPORTANT:

Citrix recommends importing one component at a time to avoid conflicts.

Automated configuration tool cmdlets for migration

This page lists all the cmdlets and parameters supported by the tool for migration usecases.

All cmdlets take parameters having one of the following types.

- String
- List of strings
- Boolean: `$true` or `$false`
- SwitchParameter: presence of the parameter means `$true`; absence of the parameter means `$false`

NOTE:

SwitchParameter is the preferred method for true or false selections but booleans are still used in the tool due to legacy issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following table is a summary of all cmdlets. See each individual section to find what parameters each cmdlet supports.

CATEGORY	CMDLET	DESCRIPTION
On-premises to cloud migration	`Export-CvadAcToFile`	Export on-premises files to YAML files.
	`Import-CvadAcToSite`	Import YAML files to the cloud. Supports create, update, and delete operations.
	`Merge-CvadAcToSite`	Import YAML files to the cloud. Supports create and update operations.
	`New-CvadAcToSite`	Import YAML files to the cloud. Supports create and update operations.
	`Sync-CvadAcToSite`	Export and import in one step.
	Granular migration For components, use parameters with commands above. Examples: `MachineCatalogs`, `Tags`. For component names, use parameters with commands above. Examples: `IncludeByName`, `ExcludeByName`.	Selectively migrate only components or component names
Cloud to cloud cmdlets	`Backup-CvadAcToFile`	Backs up all the configuration from your cloud site.
	`Restore-CvadAcToSite`	Restores backup YAML files to the cloud site. This cloud site can be the same or different than the source cloud site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	CMDLET	DESCRIPTION
	`Remove-CvadAcFromSite`	Remove component members from cloud.
	Granular migration For components, use parameters with commands above. Examples: `MachineCatalogs`, `Tags`. For component names, use parameters with commands above. Examples: `IncludeByName`, `ExcludeByName`.	Selectively migrate only components or component names
Other basic cmdlets	`Compare-CvadAcToSite`	Compares the on-premises .yml files with the cloud configuration.
Prerequisites-related cmdlets	`New-CvadAcCustomerInfoFile`	Create a customer info file.
	`Set-CvadAcCustomerInfoFile`	Update an existing customer info file.
Support and troubleshooting cmdlets	`New-CvadAcZipInfoForSupport`	Zips all log and .yml files in a single zip file to send to Citrix® for support.
	`Get-CvadAcStatus`	Use to test connectivity and to ensure that all prerequisites are met. Returns information about the tool like version number and connectivity with the cloud and connector status.
	`Test-CvadAcConnectionWithSite`	Test the connection with the cloud site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	CMDLET	DESCRIPTION
	`Find-CvadAcConnector`	Locates existing connectors and determines their running state.
	`Get-CvadAcCustomerSites`	Returns the list of all the customer sites.
	`New-CvadAcTemplateToFile`	Creates a template file for selected components.
	`Show-CvadAcDocument`	Displays this documentation in the default browser.
	`Find-CvadAcInFile`	Find in file searches component YAML files looking for members matching one or more names that may contain wildcards.
Site activation cmdlets	`Set-CvadAcSiteActiveStateOnPrem`	Sets the on-premises site state to either active or inactive.
	`Set-CvadAcSiteActiveStateCloud`	Sets the cloud site state to either active or inactive.
Merging multiple on-premises sites cmdlets	`New-CvadAcSiteMergingInfo`	Creates a site merging prefix/suffix info set.
	`Set-CvadAcSiteMergingInfo`	Updates an existing site merging prefix/suffix info set.
	`Remove-CvadAcSiteMergingInfo`	Removes an existing site merging prefix/suffix info set.

For more information on parameters and how to use them, see Granular migration parameters.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Basic cmdlets

On-premises to cloud cmdlets

- `Export-CvadAcToFile` - Export on-premises files to YAML files.

  Exports configuration from your on-premises setup. This is the default export operation for Automated configuration. No modifications are made to the on-premises site configuration. Exported files are placed in the directory *%HOMEPATH%\Documents\Citrix\AutoConfig* in a uniquely named **Export** subfolder. The folder *%HOMEPATH%\Documents\Citrix\AutoConfig* always contains the latest exported on-premises site configuration.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components		SwitchParameters
Filtering by object names	See Filtering by object names		List of strings
`TargetFolder`	Specifies the export destination folder.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`AdminAddress`	Specifies the Delivery Controller's DNS or IP address when the export is not being run on the Delivery Controller.		String
`CheckUserAndMachines`	Verifies if users and machines are in Active Directory. Users and		`$true` or `$false`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	machines that are not in Active Directory might result in import failures.		
`ZipResults`	Zips backup up YAML files into a single zip file. The file is in the same folder as the backed up YAML files and has the same name as the folder.		SwitchParameter

Returns:

- See Cmdlet return values

There are three ways of importing data into the cloud. Running specific cmdlets can result in one of the three combinations of actions on the cloud site:

- Add, Update, and Delete
- Add and Update only
- Add only

CMDLET	ADD	UPDATE	DELETE
Import	X	X	X
Merge	X	X	
New	X		

- `Import-CvadAcToSite` - Import YAML files to the cloud. Supports create, update and delete operations.

  Imports all the on-premises files to the cloud. This command ensures that the cloud end state is identical to the on-premises state. This option deletes any changes that exist in the cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Imported site configuration files are sourced from *%HOMEPATH%\Documents\Citrix\AutoConfig*. *Use with caution.*

Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`SourceFolder`	Identifies a substitute root folder for *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`Merge`	When set to `$true`, only adds components to the cloud site. Components are		`$true` or `$false`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	not removed. Set to `$false` to remove components.		
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`
`MergePolicies`	Merge policy settings and filters. Merging occurs only when a policy being imported already exists in the cloud DDC. The result of merging policies is that the cloud DDC policies contain the settings and filters it already had in addition to any new settings and filters being imported. Note that when setting and filter collisions occur, the imported values take precedence.		SwitchParameter
`OnErrorAction`	See OnErrorAction parameter.		String

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Returns:

- See Cmdlet return values

- `Merge-CvadAcToSite` - Import YAML files to the cloud. Supports create and update operations.

  Merges the on-premises files to the cloud, but does *not* delete any components in the cloud or the on-premises site. This preserves changes already made in the cloud. If a component exists in Citrix Cloud with the same name, this command can modify that component. This is the default import operation for Automated configuration. Merged site configuration files are sourced from *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`SourceFolder`	Identifies a substitute root folder for *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`Merge`	When set to `$true`, only adds components to the cloud site. Components are not removed. Set to `$false` to remove components.		`$true` or `$false`
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`
`MergePolicies`	Merge policy settings and filters. Merging occurs only when a policy being imported already exists in the cloud DDC. The result of merging policies is that the cloud DDC policies contain the settings and filters it already had in		SwitchParameter

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	addition to any new settings and filters being imported. Note that when setting and filter collisions occur, the imported values take precedence.		
`OnErrorAction`	See OnErrorAction parameter.		String

Returns:

- See Cmdlet return values

- `New-CvadAcToSite` - Import YAML files to the cloud. Supports create and update operations.

  Imports on-premises site configuration to the cloud but only adds new components. Existing cloud site components are neither updated nor deleted. Use this command if your existing cloud site components must remain unchanged.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`SourceFolder`	Identifies a substitute root folder for *%HOMEPATH%*		String

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	\Documents\Citrix\AutoConfig.		
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`OnErrorAction`	See OnErrorAction parameter.		String

Returns:

- See Cmdlet return values

- `Sync-CvadAcToSite` - Export and import in one step.

  Sync performs both an export and import in one step. Use the `SourceTargetFolder` parameter to specify the export/import destination folder.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components		SwitchParameters
Filtering by object names	See Filtering by object names		List of strings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`SourceTargetFolder`	Specifies the export/import destination folder.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`AdminAddress`	Specifies the delivery controller's DNS or IP address when the export is not being executed on the delivery controller.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`Merge`	When set to `$true`, only adds components to the cloud site. Components are not removed. Set to `$false` to remove components.		`$true` or `$false`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`
`MergePolicies`	Merge policy settings and filters. Merging occurs only when a policy being imported already exists in the cloud DDC. The result of merging policies is that the cloud DDC policies contain the settings and filters it already had in addition to any new settings and filters being imported. Note that when setting and filter collisions occur, the imported values take precedence.		SwitchParameter

Returns:

- See Cmdlet return values

Cloud to cloud cmdlets

- `Backup-CvadAcToFile` - Backs up all the configuration from your cloud site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exports your cloud configuration to .yml files. This backup can be used in a backup and restore process to restore lost components.

Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components		SwitchParameters
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`TargetFolder`	Specifies the export destination folder.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`ZipResults`	Zips backup up YAML files into a single zip file. The file is in the same folder as the backed up YAML files and has the same name as the folder.		SwitchParameter

Returns:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - See Cmdlet return values

- `Restore-CvadAcToSite` - Restores backup YAML files to the cloud site. This cloud site can be the same or different than the source cloud site.

  Restores the cloud site to the previous configuration. Imported files are sourced from the folder specified using the `-RestoreFolder` parameter, which identifies the folder containing the .yml files to restore to the cloud site. This must be a fully qualified folder specification. This cmdlet can be used for reverting to your previous configuration or for backing up and restoring your cloud site. This command can add, delete, and update your cloud site.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`RestoreFolder`	Identifies the folder containing the .yml files to restore to the cloud site. This must be a fully qualified folder specification.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of		`$true` or `$false`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	the cmdlet. Set to `$false` to suppress the log display.		
`Merge`	When set to `$true`, only adds components to the cloud site. Components are not removed. Set to `$false` to remove components.		`$true` or `$false`
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`
`MergePolicies`	Merge policy settings and filters. Merging occurs only when a policy being imported already exists in the cloud DDC. The result of merging policies is that the cloud DDC policies contain the settings and filters it already had in addition to any new settings and filters		SwitchParameter

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	being imported. Note that when setting and filter collisions occur, the imported values take precedence.		
`OnErrorAction`	See OnErrorAction parameter.		String

Returns:

- See Cmdlet return values

- `Remove-CvadAcFromSite` – Remove component members from cloud.

  Can reset the entire site or remove member items from a component (For example, removing one machine catalog from the list of catalogs). This can be used when coupled with the `IncludeByName` parameter to selectively remove specific members.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components		SwitchParameters
Filtering by object names	See Filtering by object names		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to		`$true` or `$false`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	suppress the log display.		

Returns:

- See Cmdlet return values

Other basic cmdlets

- `Compare-CvadAcToSite` - Compares the on-premises .yml files with the cloud configuration, producing a report of changes that are made by an `Import`, `Merge`, or `Restore` cmdlet.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components.		SwitchParameters
Filtering by object names	See Filtering by object names.		List of strings
Cloud-accessing parameters	See Cloud-accessing parameters.		SwitchParameters
`SourceFolder`	Identifies a substitute root folder for *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Specifies the language of human-readable text that can be exported.		String
`Quiet`	Suppress logging to the console.		SwitchParameter

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true` or `$false`
`Merge`	When set to `$true`, only adds components to the cloud site. Components are not removed. Set to `$false` to remove components.		`$true` or `$false`
`AddOnly`	When set to `$true`, adds only new components, does not update or delete existing components. Set to `$false` to allow updates and deletions. `Merge` is ignored when this parameter is `$true`.		`$true` or `$false`
`OnErrorAction`	See OnErrorAction parameter.		String

Returns:

- See Cmdlet return values

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Granular migration parameters

Migrate by components

The following components can be specified with cmdlets supporting them. The `All` option is automatically selected when no component parameters are specified. To avoid errors, we recommend that you migrate components in the following order:

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

Filtering by object names

Migrate by component names

The `IncludeByName` and `ExcludeByName` parameters enable including and excluding component members in cmdlets by name. Only one component (for example, delivery groups) can be chosen at a time in any of the supported cmdlets. If a component member is in both areas, exclude overrides any other parameter and an entry is made in the log fixup list identifying the component and member name that was excluded.

`IncludeByName` and `ExcludeByName` take a list of component member names. Any name can contain one or more wildcards. Two types of wildcards are supported. The list of component member names must be enclosed in single-quotes when any member name contains special characters.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- * Matches any number of characters
- ? Matches a single character

`IncludeByName` and `ExcludeByName` can also take a file containing a list of members where each member can be explicit or contain wildcards. Each line in the file can contain one member. Leading and trailing spaces are trimmed from the member name. The file name must be preceded by the @ sign and be surrounded by single quotes (a PowerShell requirement so the @ is not reinterpreted). Multiple files can be listed in addition to being mixed with member names.

One example of merging all delivery groups whose names begin with `DgSite1` and contain `Home2` would be written:

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

By Delivery Group Name

`ByDeliveryGroupName` filters by the delivery group name for applications and application groups. This parameter is always an inclusion list identifying members to include based on their delivery group association.

`ByDeliveryGroupName` takes a list of delivery group names. Any name can contain one or more wildcards. Two types of wildcards are supported.

- * matches any number of characters
- ? matches a single character

The following example merges all applications that reference all delivery group names beginning with `EastDg`.

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

Exclude Disabled

`ExcludeDisabled` filters out from import operations all applications and application groups that are disabled. `ExcludeDisabled` defaults to `false`, meaning all applications and application groups are imported regardless of their enabled state.

By Machine Name

`ByMachineName` filters by the machine name for machine catalogs and delivery groups. This parameter is always an inclusion list identifying members to include based on their machine name association.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`ByMachineName` takes a list of machine names where any name can contain one or more wildcards. Two types of wildcards are supported.

- * matches any number of characters
- ? matches a single character

When exporting or importing and using `ByMachineName` and a machine name filter results in no machines in the machine catalog or delivery group, the machine catalog or delivery group is excluded from the export or import.

NOTE:

Use of `ByMachineName` in any import type cmdlet results in `MergeMachines` being set to `$true`.

Merge Machines

`MergeMachines`, when set to `$true`, instructs the import operation to add machines only to the machine catalog or delivery group. Machines are not removed, allowing for incremental additive operations.

`MergeMachines` defaults to false meaning machines are removed if they are not present in the machine catalog or delivery group .yml file. `MergeMachines` is set to `$true` when `ByMachineName` is used but can be overridden by setting `MergeMachines` to false.

Prerequisites-related cmdlets

- `New-CvadAcCustomerInfoFile` - Create a customer info file. By default, the customer info file is located at *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
`CustomerId`	Customer's ID.	x	String
`ClientId`	Customer's client ID created on Citrix Cloud. The CustomerId and Secret must be specified when	Conditionally	String

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	using this parameter.		
`Secret`	Customer's secret key created on Citrix Cloud. The CustomerId and ClientId must be specified when using this parameter.	Conditionally	String
`Environment`	Production, ProductionGov, or ProductionJP environment.		Enumeration
`LogFileName`	Change the log file prefix from CitrixLog to something else.		String
`AltRootUrl`	Use only under the direction of Citrix.		String
`StopOnError`	Stops the operation upon first error.		`$true` or `$false`
`TargetFolder`	Use the specified folder as the root folder instead of *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Use the specified local instead of the locale derived from the system the tool is run on.		String

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
`Editor`	Use the specified editor to display the log at the completion of each cmdlet. Notepad.exe is the default editor. This parameter must include the fully qualified file specification to the editor and the editor must take the log file spec as its only parameter.		String
`SecurityCsvFileSpec`	The fully qualified file specification pointing to the SecurityClient.csv file downloaded from Citrix Identity and Access Management. The CustomerId must be specified when using this parameter.		String

Returns:

- See Cmdlet return values

- `Set-CvadAcCustomerInfoFile` - Update an existing customer info file. Only cmdlet specified parameters are changed. All unspecified parameter values in the CustomerInfo.yml file are unchanged.

  Parameters:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
`CustomerId`	Customer's ID.		String
`ClientId`	Customer's client ID created on Citrix Cloud.		String
`Secret`	Customer's secret key created on Citrix Cloud.		String
`Environment`	Production, ProductionGov, or ProductionJP environment.		Enumeration
`LogFileName`	Change the log file prefix from CitrixLog to something else.		String
`StopOnError`	Stops the operation upon first error.		`$true` or `$false`
`TargetFolder`	Use the specified folder as the root folder instead of *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Use the specified local instead of the locale derived from the system the tool is run on.		String
`Editor`	Use the specified editor to display the log at the completion of each cmdlet. Notepad.exe is the		String

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	default editor. This parameter must include the fully qualified file specification to the editor and the editor must take the log file spec as its only parameter.		
`SecurityCsvFileSpec`	The fully qualified file specification pointing to the SecurityClient.csv file downloaded from Citrix Identity and Access Management. The CustomerId must be specified when using this parameter.		String

Returns:

- See Cmdlet return values

Prerequisites-related parameters

Along with the cloud accessing parameters, the following parameters can be used with the prerequisites-related cmdlets:

- `Environment` – Production or ProductionGov environment.
- `LogFileName` – Change the log file prefix from CitrixLog to something else.
- `StopOnError` – Stops the operation upon first error.
- `AlternateRootFolder` – Use the specified folder as the root folder instead of *%HOMEPATH%\Documents\Citrix\AutoConfig*.
- `Locale` – use the specified local instead of the locale derived from the system the tool is run on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Editor` – use the specified editor to display the log at the completion of each cmdlet. Notepad.exe is the default editor. This parameter must include the fully qualified file specification to the editor and the editor must take the log file spec as its only parameter.

Support and troubleshooting cmdlets

- `New-CvadAcZipInfoForSupport` - Zips all log and .yml files in a single zip file to send to Citrix for support. Customer sensitive information (CustomerInfo.yml and CvadAcSecurity.yml) is not included in the zip. The Icon.yml file is also excluded due to its size. The zip file is placed in *%HOMEPATH%\Documents\Citrix\AutoConfig* and named *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, based on the date and timestamp. This zip file can also act as a backup.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
`TargetFolder`	Specifies a target folder to create and save the zip file.		String
`Quiet`	Suppress logging to the console.		SwitchParameter

  Returns:

  - Zip file with zip file name and location is displayed on the command prompt.

- `Get-CvadAcStatus` - Use to test connectivity and to ensure all prerequisites are met. Returns information about the tool like version number and connectivity with the cloud and connector status.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`SiteId`	Identifies the site to connect to.		String

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
`AdminAddress`	This is the DNS or IP address of the on-premises Delivery Controller used to verify the admins access level. This is required if the tool is not being run on a Delivery Controller.		String

Returns:

- Displays the results for each item.

- `Test-CvadAcConnectionWithSite` – Test the connection with the cloud site to verify that the communication connection is working. This cmdlet uses the cloud accessing parameters or the CustomerInfo.yml file to specify the customer connection information.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`Quiet`	Suppress logging to the console.		SwitchParameter

  Returns:

  - Test results are displayed on the command line.

- `Find-CvadAcConnector` - Locates existing connectors and determines their running state. This cmdlet uses information from the CustomerInfo.yml file or the customer ID parameter to locate the customer's connectors.

  Parameters:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
`CustomerInfoFileSpec`	The file specification pointing to a customer information file to override the default location and name. This parameter is ignored when the `CustomerId` parameter is provided.		String
`CustomerId`	The customer's ID. This parameter overrides the same value in the CustomerInfo.yml file.		String

Returns:

- Results are shown on the command line.

- `Get-CvadAcCustomerSites` - Returns the list of all the customer sites. This cmdlet uses the cloud accessing parameters or the CustomerInfo.yml file to specify the customer connection information.

  Parameters:

  - See Cloud-accessing parameters

  Returns:

  - Displays a list of found customer site IDs.

- `New-CvadAcTemplateToFile` – Creates a template file for selected components, allowing you to manually create an import file.

  Parameters:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components		SwitchParameters
`TargetFolder`	Specifies the export destination folder.		String

Returns:

- See Cmdlet return values

- `Show-CvadAcDocument` - Displays this documentation in the default browser.

  Parameters:

  - None.

  Returns:

  - Display this webpage in the default web browser.

- `Find-CvadAcInFile` - Find in file searches component YAML files looking for members matching a one or more names that may contain wildcards. The result is a report of found members. Find in file can only search one component at a time. Find in file searches all YAML files in the current folder and all subfolders. Use `FindSourceFolder` to limit the number of files to search.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Migrate by components	See Migrate by components. Note: The `-All` value is not valid.		SwitchParameters
`IncludeByName`	A list specifying the names of delivery groups to include when setting the site active state to active. The '*' and '?' wildcards are		List of strings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	supported in names.		
`Unique`	Report only unique-found members.		SwitchParameter
`IncludeYaml`	Include the member specific YAML.		SwitchParameter
`FindSourceFolder`	The folder find begins searching in.		String
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		SwitchParameter
`Quiet`	Suppress logging to the console.		SwitchParameter

Return:

- Creates a report containing found members for the specified component.

Site activation cmdlets

For more information on activating sites and the usage of these cmdlets, see Activating sites.

- `Set-CvadAcSiteActiveStateOnPrem` - Sets the on-premises site state to either active or inactive.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
`SiteActive`	When present, sets the on-premises site to active removing the maintenance mode from all delivery groups. When this parameter is not present, maintenance mode is set on all delivery groups.		SwitchParameter
`IncludeByName`	A list specifying the names of delivery groups to include when setting the site active state to active. The '*' and '?' wildcards are supported in names.		List of strings
`ExcludeByName`	A list specifying the names of delivery groups to exclude when setting the site active state to active. The '*' and '?' wildcards are supported in names.		List of strings
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to		`$true or $false`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	suppress the log display.		

Returns:

- See Cmdlet return values

- `Set-CvadAcSiteActiveStateCloud` - Sets the cloud site state to either active or inactive.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
Cloud-accessing parameters	See Cloud-accessing parameters		SwitchParameters
`SiteActive`	When present, sets the cloud site to active removing the maintenance mode from all delivery groups. When this parameter is not present, maintenance mode is set on all delivery groups.		SwitchParameter
`IncludeByName`	A list specifying the names of delivery groups to include when setting the site active state to active. The '*' and '?' wildcards are supported in names.		List of strings
`ExcludeByName`	A list specifying the names of delivery groups to exclude		List of strings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
	when setting the site active state to active. The '*' and '?' wildcards are supported in names.		
`Quiet`	Suppress logging to the console.		SwitchParameter
`DisplayLog`	Displays the log file at the completion of the cmdlet. Set to `$false` to suppress the log display.		`$true or $false`

Returns:

- See Cmdlet return values

Merging multiple on-premises sites cmdlets

For more information on site merging and usage of these cmdlets, see Merge multiple sites into a single site.

- `New-CvadAcSiteMergingInfo` - Creates a site merging prefix/suffix info set. It is not necessary to know all prefixes or suffixes at the beginning. They can be updated with `Set-CvadAcSiteMergingInfo` or by manually editing the SiteMerging.yml file. Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
`SiteName`	The name used to identify the set of prefixes/suffixes for a specific site. It can match the name of the actual site but does not need to.	x	String

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME	DESCRIPTION	REQUIRED?	TYPE
Site merging parameters	See Site merging parameters		SwitchParameters
`Quiet`	Suppress logging to the console.		SwitchParameter

Returns:

- None

- `Set-CvadAcSiteMergingInfo` - Updates an existing site merging prefix/suffix info set.

  Parameters:

NAME	DESCRIPTION	REQUIRED?	TYPE
`SiteName`	The name used to identify the set of prefixes/suffixes for a specific site. It can match the name of the actual site but does not need to.	x	String
Site merging parameters	See Site merging parameters		SwitchParameters
`Quiet`	Suppress logging to the console.		SwitchParameter

  Returns:

  - None

- `Remove-CvadAcSiteMergingInfo` - Removes an existing site merging prefix/suffix info set.

  Parameters:

  - `SiteName` – identifies the set of site prefixes and suffixes. This is a string and is required.

  Returns:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- None

Site merging parameters

The following parameters can be used when running the site merging cmdlets. All listed parameters are strings.

- `SiteName` –the name used to identify the set of prefixes/suffixes for a specific site. It can match the name of the actual site but does not need to. SiteName is a required parameter.
- `AdminScopedPrefix` – the prefix to apply to administrator scopes.
- `ApplicationPrefix` - the prefix to apply to applications.
- `ApplicationFolderPrefix` – the prefix to apply to application folders; `ApplicationFolderPrefix` can be combined with `ApplicationFolderRoot`.
- `ApplicationFolderRoot` – the new root folder to application folders. This creates an extra folder hierarchy. `ApplicationFolderRoot` can be combined with `ApplicationFolderPrefix`.
- `ApplicationGroupPrefix` – the prefix for application groups.
- `ApplicationUserPrefix` – the prefix to apply to the application name the user sees.
- `ApplicationAdminPrefix` – the prefix to apply to the application name the administrator sees.
- `DeliveryGroupPrefix` – the prefix to apply to delivery groups.
- `GroupPolicyPrefix` – the prefix to apply to policy names.
- `HostConnectionPrefix` – the prefix to apply to host connections.
- `MachineCatalogPrefix` – the prefix to apply to machine catalogs.
- `StoreFrontPrefix` – the prefix to apply to StoreFront™ names.
- `TagPrefix` – the prefix to apply to tags.
- `AdminScopedSuffix` – the suffix to apply to administrator scopes.
- `ApplicationSuffix` - the suffix to apply to applications.
- `ApplicationFolderSuffix` – the suffix to apply to application folders; `ApplicationFolderSuffix` can be combined with `ApplicationFolderRoot`.
- `ApplicationGroupSuffix` – the suffix for application groups.
- `ApplicationUserSuffix` – the suffix to apply to the application name the user sees.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `ApplicationAdminSuffix` – the suffix to apply to the application name the administrator sees.
- `DeliveryGroupSuffix` – the suffix to apply to delivery groups.
- `GroupPolicySuffix` – the suffix to apply to policy names.
- `HostConnectionSuffix` – the suffix to apply to host connections.
- `MachineCatalogSuffix` – the suffix to apply to machine catalogs.
- `StoreFrontSuffix` – the suffix to apply to StoreFront names.
- `TagSuffix` – the suffix to apply to tags.
- `SiteRootFolder` – the fully qualified folder name to use for exports and imports; this can be a local folder or a file share.

Generic parameters

Cloud accessing parameters

All cmdlets accessing the cloud support the following extra parameters.

NOTE:

The CustomerId, ClientId, and Secret can be placed in the CustomerInfo.yml file or specified with the cmdlet using the following parameters. When they are specified in both places, the cmdlet parameters take precedence.

- `CustomerId` – The customer ID used in the Rest APIs and is required to access all Rest APIs. Your customer ID is found in Citrix Cloud.
- `ClientId` – The clientID created on the Citrix Cloud Identity and Access Management website. This is required to obtain the bearer token needed for authentication for all Rest APIs.
- `Secret` – The secret key created on the Citrix Cloud Identity and Access Management website. This is required to obtain the bearer token needed for authentication for all Rest APIs.
- `CustomerInfoFileSpec` – The file specification pointing to a customer information file to override the default location and name.

Migration mode parameters

Cmdlets modifying the cloud site configuration (`Import` , `Restore` , `Merge` , `New` , and `Sync`) support the following extra parameters to provide further flexibility.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `CheckMode` – Performs the import operation but makes *no* changes. All expected changes are reported before the import completes. You can use this command to test your import before it occurs.
- `BackupFirst` – Backs up the cloud contents to .yml files before modifying the cloud configuration. This is enabled by default.
- `Confirm` – When true, prompts users to confirm that they want to make changes to the cloud site configuration. The `Remove` cmdlet shows a prompt due to its destructive nature. Set to false if no prompt is desired, such as running inside automated scripts. `Confirm` defaults to true.
- `SecurityFileFolder` – This is the fully qualified folder containing the CustomerInfo.yml file which might point to a local folder or a network share folder that may be under authentication control. The tool will not prompt for credentials; access to the controlled resource must be obtained before running the tool.
- `SiteName` – Specifies the site merging prefix and suffix set to use when importing.
- `SiteActive` – Specifies whether the imported site is active or inactive. By default, this parameter is set to `$false` meaning the imported site is inactive.

Log display parameters

The `Export`, `Import`, `Sync`, `Restore`, `Backup`, `Compare`, and `Remove` cmdlets display the log file when the operation completes. You can suppress the display by setting the `-DisplayLog` parameter to `$false`. Notepad.exe is used by default to display the log file. You can specify a different editor in the CustomerInfo.yml file.

`Editor: C:\Program Files\Notepad++\notepad++.exe`

Cmdlet return values

ActionResult

All cmdlets return the following value.

```
public class ActionResult

{

    public bool                         Overall_Success;

    public Dictionary&lt;string, string>   Individual_Success;
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    public object                       CustomResult;

}
```

`Overall_Success` returns a single boolean showing the overall success of the cmdlet across all selected components: true meaning successful and false meaning unsuccessful.

`Individual_Success` returns one or three values for each main component. A component's result can be Success, Failure, or Skipped. Skipped indicates that the component was not selected for execution by the cmdlet.

`CustomResult` is cmdlet specific.

CustomResult

`Import`, `Merge`, `Restore`, `Sync`, `Compare`, `Compare File`, and `Remove` return the following custom result information to a single instance of `EvaluationResultData`.

NOTE:

`Export` and `Template` cmdlets do not return a custom result.

```
 public class EvaluationResultData

 {

     public Dictionary&lt;string, Dictionary&lt;string, ActionResultValues
>> EvaluationResults;

     public int                  Added;

     public int                  Updated;

     public int                  Deleted;

     public int                  NoChange;

     public int                  TotalChanged;

     public EvaluationResults     OverallResult;
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    public string               CloudBackupFolder;

    public string               SourceBackupFolder;

 }

 Where:

 public enum ActionResultValues

{

    Add,

    Update,

    Delete,

    Identical,

    DoNothing

 }

 public enum EvaluationResults

 {

    Success,

    Failure,

    Skipped

 }
```

`EvaluationResults` displays a list with one entry per selected component. The key is the component name and the value is a list of each component member and the action taken on that component member. Actions can be any one of the `ActionResultValues` values.

`Added`, `Updated`, `Deleted`, and `NoChange` indicate that the total number of component members added, updated, deleted, or no action taken, in that order.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`TotalChanged` is the sum of `Added`, `Updated`, and `Deleted`.

`OverallResult` is a single boolean indicating the result of the cmdlet. True indicates total success across all components and false indicates failure in processing one or more components.

`CloudBackupFolder` is the fully qualified file specification of the cloud site configuration backup before the cmdlet performing any cloud-modifying actions.

`SourceBackupFolder` is the fully qualified file specification of the source file backup made after completion of the cmdlet. By default, these files are at *%HOMEPATH%\Documents\Citrix\AutoConfig*.

PowerShell help

PowerShell help is available for each cmdlet. All parameters are documented with each cmdlet along with a brief explanation of the cmdlet. To access help for any cmdlet, type `Get-Help` in front of the cmdlet.

```
Get-Help Import-CvadAcToSite
```

Automated configuration tool cmdlets for backup and restore

This page lists all the cmdlets and parameters supported by the tool to trigger the backup and restore APIs that Studio uses.

Backup storage cmdlets

Get-BckRstrStorage

This cmdlet is applicable to only on-premises. Gets details for the storage where backups are saved.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.

Set-BckRstrStorage

This cmdlet is applicable to only on-premises. Sets a new storage where backups are saved.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
	parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`MaximumBackups`	The maximum number of unpinned backups to be persisted until the backup cleanup process removes the oldest backups when new backups are created.
`MaximumPinnedBackups`	The maximum number of pinned backups to be persisted. These backups are not removed by the cleanup process.
`BlobStorageType`	The type of storage: `FileStorage` or `CustomerAzureStorage`.
`FileStoragefolder`	The fully qualified folder specification for the `BlobStorageType` `FileStorage` option.
`Info1`	For `FileStorage`, optional `UserName` For `CustomerAzureStorage`, the Azure SAS URL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`Info2`	For `FileStorage`, optional Password
`Info3` and `Info4`	Not used

Test-BckRstrStorage

This cmdlet is applicable to only on-premises. Tests to determine that the defined storage is valid.

For `FileStorage`, the test verifies that the folder exists and can be written to.

For `CustomerAzureStorage`, the test verifies that the SAS URL has the correct permissions and the current date is with the URL's start and end date.

Returns `true` if valid and `false` if invalid.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`Quiet`	The parameter to suppress output to the console.

Back up cmdlets

Get-BckRstrBackups

Enumerates backups stored in the Backup or Restore blob storage location. For Citrix Virtual Apps and Desktops™, this location is set up by the administrator through WebStudio. For DaaS, this is the pre-existing customer Azure storage. Use `Get-BckRstrBackupsWithDetiails` for complete information about each backup. Backup details include the following:

- Backup Name
- Notes
- Pinned (true or false)
- Date and time of backup
- History UID
- Related UID (UID of last Restore history record)
- Related Date and time
- Related if run in check-mode
- Duration in seconds
- Administrator name
- Details enumerating each component and count of members in each component.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.

Get-BckRstrBackupsMembers

Enumerates a single component's members stored in a selected backup. Member names are returned in a simple list.

The components are:

- Tags
- AdminScopes
- AdminRoles
- AdminAdministrators (on-premises only)
- HostConnections
- Icons
- AdminFolders
- MachineCatalogs
- StoreFronts
- DeliveryGroups
- ApplicationGroups
- ApplicationFolders

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Applications
- AppVServers
- AppLibPackageDiscovery
- AppVIsolationGroups
- GroupPolicies
- UserZonePreferences
- SiteData
- Zones (on-premises only)

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`BackupName`	The name of backup. The `.zip` extension is optional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`Component`	The components to be included in backup.

New-BckRstrBackup

Starts a new backup action on the Delivery Controller. This action is asynchronous to the `New-BckRstrBackup` cmdlet.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`Notes`	The notes about the backup.
`PollForCompletion`	The parameter to poll the action running on the Delivery Controller until the action completes. The polling logs progress and completion

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
	results to the console unless the `Quite` parameter is specified.

Pin backups cmdlets

Set-BckRstrPinBackups

Pins a backup so it is not removed as part of the Delivery Controller backup cleaning process.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`BackupName`	The name of backup. The `.zip` extension is optional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set-BckRstrUnpinBackups

Unpins a backup so it is available to be removed in the Delivery Controller backup cleaning process.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`BackupName`	The name of backup. The `.zip` extension is optional.

Remove backup cmdlet

Remove-BckRstrBackup

Removes one or more backups.

Parameters:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`IncludeByName`	The filter to specify which component members to consider for restore. This is a comma separated list of filter values and can have the wildcard characters `*` and `?`.

Scheduled backups cmdlets

Get-BckRstrSchedules

Gets a list of backup schedules.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`BackupName`	The name of backup. The `.zip` extension is optional.
`Notes`	The notes to set or change.

New-BckRstrSchedule

Creates a new backup schedule.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`Name`	The schedule name.
`Frequency`	The type of frequency: Daily, Weekly, or Monthly.
`Day`	If the frequency is daily.
`DaysInWeek`	If the frequency is weekly.
`DayInMonth`	If the frequency is monthly.
`WeekInMonth`	If the frequency is monthly.
`StartDate`	The format is `M/d/yy`
`StartTime`	The start time specified as a 24 hour clock.
`FrequencyFactor`	Run every n times such as every day (value = 1) or every other day (value = 2)
`Description`	The description of the scheduled backup

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`Enabled`	The parameter to enable this backup schedule. `True` when enabled and `false` when disabled
`TimeZoneId`	The Windows Time Zone Id

Set-BckRstrSchedule

Modifies an existing backup schedule. Provide the name or Uid to select the schedule to modify.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`Name`	The schedule name.
`Uid`	If the schedule name is to be changed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`Frequency`	The type of frequency: Daily, Weekly, or Monthly.
`Day`	If the frequency is daily.
`DaysInWeek`	If the frequency is weekly.
`DayInMonth`	If the frequency is monthly.
`WeekInMonth`	If the frequency is monthly.
`StartDate`	The format is `M/d/yy`
`StartTime`	The start time specified as a 24 hour clock.
`FrequencyFactor`	Run every n times such as every day (value = 1) or every other day (value = 2)
`Description`	The description of the scheduled backup
`Enabled`	The parameter to enable this backup schedule. `True` when enabled and `false` when disabled
`TimeZoneId`	The Windows Time Zone Id

Set-BckRstrScheduleEnabled

Enables an existing backup schedule. Provide the name or Uid to select the schedule to enable.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`Name`	The schedule name.
`Uid`	If the schedule name is to be changed.

Set-BckRstrScheduleDisabled

Disables an existing backup schedule. Provide the name or Uid to select the schedule to disable.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`Name`	The schedule name.
`Uid`	If the schedule name is to be changed.

Limit backups cmdlet

Set-BckRstrOptions

Limits scheduled backups to one per day to avoid identical backups.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
	Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`OneScheduledBackupPerDay`	The parameter to limit scheduled backups to one per day to avoid identical backups.

Restore cmdlet

Restore-BckRstrBackups

Restores members from a single component from an existing backup.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`BackupName`	The name of backup. The `.zip` extension is optional.
`Component`	The components to be included in backup.
`Notes`	The notes about the backup.
`CheckMode`	The parameter to identify component members that would be restored but does not perform the actual restore.
`RestoreType`	The restore type: MissingOnly or MissingUpdateExisting
`IncludeByName`	The filter to specify which component members to consider for restore. This is a comma separated list of filter values and can have the wildcard characters `*` and `?`.

History cmdlets

Get-BckRstrHistory

Gets a list history details for all actions.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.

Get-BckRstrSpecificBackupHistory

Gets a list of history details for a specific backup.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
	Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	The parameter to suppress output to the console.
`BackupName`	The name of backup. The `.zip` extension is optional.

Set-BckRstrNotes

Sets or changes the notes in a history record.

Parameters:

PARAMETER	DESCRIPTION
`CustomerId`	The customer ID needed to obtain a bearer token.
`CientId`	The client ID needed to obtain a bearer token.
`Secret`	The secret needed to obtain a bearer token.
`CustomerInforFileSpec`	The fully qualified file specification of the customer info file containing security and environment information.
`ProfileName`	The parameter to identify an existing security profile used in place of the previous parameters. See XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud for how to set security profiles.
`Environment`	The type of production environment: Production, ProductionGov, ProductionJP, OnPrem.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
`Quiet`	The parameter to suppress output to the console.
`BackupName`	The name of backup. The `.zip` extension is optional.
`Notes`	The notes to set or change.

Troubleshoot Automated configuration and additional information

IMPORTANT:

For commonly occurring error messages for Automated configuration and corresponding solutions, see the *troubleshooting FAQ* at Knowledge Center article CTX277730.

Automated configuration tool errors

Automated configuration tool operations can sometimes produce errors. When this happens failures can occur when processing components like Machine Catalogs, Delivery Groups, or Group Policies, for example. Using `OnErrorAction` and continuation parameters allows you to catch errors mid-processing, resolve them, and pick up where you left off.

The default `OnErrorAction` value is `StopCompEnd`. When an error occurs, the tool finishes processing the current component. No additional components are processed, and errors do not carry forward to downstream, dependent components. After you resolve any errors, you can rerun your cmdlets with any continuation parameter applied.

OnErrorAction parameter

You can define `OnErrorAction` parameter values on migration commands to control how the tool responds to errors that it finds when processing components.

This table shows parameter values and their descriptions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VALUE	DESCRIPTION
`Continue`	Attempts to process as many of all components as possible.
`Pause`	Pauses at the end of processing and prompts you to continue or stop.
`StopCompEnd`	Attempts to process as much of the component as possible. Stops after the component is finished. (Default)
`StopImmediately`	Processing stops when an error is found.

Migration cmdlets

You can apply the `OnErrorAction` parameter to the following migration commands:

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

Example: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

Resume parameters

These parameters define how the tool resumes after an operation pauses or stops because of an error.

You can apply resume parameters to migration cmdlets that include one of the following `OnErrorAction` parameter values:

- `Pause`
- `StopCompEnd`
- `StopImmediately`

This table shows parameter values and their descriptions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VALUE	DESCRIPTION
`-AllRemaining`	Requires a starting component. Processing begins at the starting component and processes all remaining components. Multiple components are processed.
`-Resume`	Uses the component from `CurrentComponent.txt` as the starting point. All remaining is set to true. Multiple components are processed.
`-Repeat`	Uses the component from `CurrentComponent.txt` as the starting point. All remaining is set to false. Only one component is processed.

The last component processed is stored in the `CurrentComponent.txt` file in the AutoConfig folder. Editing this file is not recommended. If you specify `-Resume` or `-Repeat`, and `CurrentComponent.txt` is missing or invalid, processing stops, and you are prompted to select a component.

Setting the OnErrorAction in the CustomerInfo.yml file

You can also set `OnErrorAction` values in the `CustomerInfo.yml` file. Set the values using the following cmdlets:

- For a new file: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- For an existing file: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

Logs

Running any cmdlet results in a log file creation and an entry in the main history log file. All operation log files are placed in a backup folder. All log file names begin with `CitrixLog`, then show the auto-config operation and the date and timestamp of the cmdlet execution. Logs do not auto-delete.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The main history log is located in `*%HOMEPATH%\Documents\Citrix\AutoConfig*`, in the file named **History.Log**. Each cmdlet execution results in a main log entry containing the date, operation, result, backup, and log file locations of the execution.

You can also use the `New-CvadAcZipInfoForSupport` cmdlet to collect logs to send to Citrix for support. This cmdlet zips all log and .yml files in a single zip file. Customer sensitive information (CustomerInfo.yml and CvadAcSecurity.yml) is not included in the zip. The Icon.yml file is also excluded due to its size. The zip file is placed in *%HOMEPATH%\Documents\Citrix\AutoConfig* and named *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, based on the date and timestamp. This zip file can also act as a backup.

Each log file includes the following:

- The name of the operation and whether the check mode is enabled
- The start and end date and time
- Multiple entries for each component's actions and success/failure notifications
- Summary of actions taken including various counts of created objects
- Suggested fixes where applicable
- Backup folder location where applicable
- Main log location
- Duration

Diagnostic files

Diagnostic files assist you in determining and resolving problems. The following files are created when their operation is run. They are located in the action-specific subfolder under *%HOMEPATH%\Documents\Citrix\AutoConfig*. Include these files when providing information for problem resolution support.

Export

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

This file counts all Broker PowerShell SDK calls made to export the site configuration to files.

Import, Merge, Restore, Sync, Backup, Compare

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

This file documents each Rest API call and related information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

This file contains the all `Add`, `Update`, and `Delete` Rest API content.

Problems resulting from dependencies

Imports and merges might fail due to missing dependencies. Some common problems are:

1. Group Policies are missing delivery group filters. The usual causes are delivery groups that have not been imported.
2. Applications fail to import or merge. The usual cause is missing delivery groups or application groups that have not been imported.
3. Application groups are missing a RestrictToTag. The usual causes are tags that have not been imported.
4. Host connections fail. The usual cause is missing security information in the CvadAcSecurity.yml file.
5. Machine catalogs fail. The usual cause is host connections that were not imported.
6. Machines missing from machine catalogs and delivery groups. The usual cause is machines that were not found in Active Directory.
7. Users missing from delivery groups. The usual cause is users that were not found in Active Directory.

Recommendations

- Do not run more than one instance of Automated configuration at a time. Running multiple concurrent instances produces unpredictable results in the cloud site. If this occurs, rerun one instance of Automated configuration to bring the site to the expected state.
- Do not work or change data in Studio while running Automated configuration.
- Always visually verify the merge or import or restore results in Studio to ensure that the cloud site meets expectations.

Folders

Default folder root location

All Automated configuration tool operations occur in the root folder or in subfolders inside it. The root folder is located in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Export

All exported files are placed in two folder locations, providing ease-of-use and a history of exports. Exports are always placed in the root folder. Copies are placed in a subfolder named **Export** with the date and time of the export.

The root folder always contains the most recent exported on-premises site configuration. Each **Export** subfolder contains the export done on the indicated date and time, which maintains a history of exports. You can use any **Export** subfolder to configure the cloud site. Automated configuration does not delete or modify existing export subfolders.

Import/Merge/Sync/Compare

`Import`, `Merge`, and `Compare` operations always sourced from files located in the root folder. Each operation results in the creation of a subfolder to which files in the root folder are copied, providing a history of cloud site changing source files.

Restore

The `Restore` operation uses an existing subfolder to configure the cloud site. The source folder is specified on the required `-RestoreFolder` parameter. Unlike with other commands, no new subfolder is created because the `Restore` operation uses an existing subfolder. The restore folder can be the root folder but still must be specified on the `-RestoreFolder` parameter.

Backups

Automated Configuration initializes, updates, and backs up a cloud site configuration. When used over time, many different configurations can change on the cloud site. To facilitate long-term use and preserve history changes, Automated Configuration uses a preservation scheme to save this history of changes and provide a method to restore earlier states.

Cloud site configuration backups are always made to a subfolder named **Backup** with the data and time of the backup. Automated Configuration does not delete or modify existing export subfolders.

You can use the backups to restore specific components or your entire configuration. To restore the entire delivery group and machine catalog components, use the cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig/
Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The backup file information in the preceding cmdlet is based on your own backups.

To restore the entire cloud site configuration, use the cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss
```

NOTE:

The backup file information in the preceding cmdlet is based on your own backups.

Changing the default root folder

The `Export`, `Import`, `Merge`, `Sync`, and `Compare` operations can change the default root folder by using the `–AlternateFolder` parameter. The creation and management of per-operation subfolders remains the same as previously described.

Files copied to subfolders

All files having an ".yml" extension are copied to operation subfolders except for the following:

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

Automated fail-safe cloud site backups

A backup of the current cloud site configuration is made before running operations that change the configuration. This includes `Import`, `Merge`, `Sync`, and `Restore` parameters. The backup is always in a subfolder beneath the operational subfolder.

In the case of `Restore`, the backup folder is a subfolder of the folder specified on the `-RestoreFolder` parameter.

Automation

Automated configuration tool cmdlets can be run in automation scripts without administrator intervention by suppressing prompts and the display of the log results at cmdlet completion. You can also set parameters to do the same by using the CustomerInfo.yml file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add the following parameter to cloud modifying cmdlets to suppress the display of prompts.

`-Confirm $false`

Add the following parameter to cmdlets to suppress the display of log at the completion of the cmdlet.

`-DisplayLog $false`

Add the following parameter to cmdlets to suppress logging to the PowerShell command window.

`-Quiet`

As another method, the following parameters can be placed in the CustomerInfo.yml file.

`Confirm: False`

`DisplayLog: False`

Exporting from PCs other than the Delivery Controller™

The Automated configuration tool uses multiple Citrix PowerShell SDKs to export the on-premises site configuration to files. These SDKs are automatically installed on the Delivery Controller, enabling the tool to run on the Delivery Controller without extra actions. When running on non-Delivery Controller machines, it is necessary to install the set of Citrix PowerShell SDKs needed by the tool. This SDK set is part of Citrix Studio which can be installed from the Citrix Virtual Apps and Desktops™ installation media.

NOTE:

Automated configuration cannot be run on the Cloud Connector.

Moving to Citrix Cloud™ Government and Japan Control Plane

The Citrix Cloud Government and Japan Control Plane environments use different access points to authenticate and allocate access tokens. This unique requirement applies to any Automated configuration tool accessing the cloud. Perform the following steps to use Automated configuration in these environments.

1. In the *%HOMEPATH%\Documents\Citrix\AutoConfig* folder, edit CustomerInfo.yml.
2. Add one of the following lines, depending on the environment you want to connect to, to CustomerInfo.yml (or change it, if already present.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`Environment: 'ProductionGov'`

or

`Environment: 'ProductionJP'`

Automated Configuration is now able to be used on these environments.

Citrix Cloud data collection

For information on what information Citrix Cloud collects, see Citrix Cloud Services Customer Content and Log Handling.

Additional resources

Discussion forum

Visit the Citrix Discussion forum for Automated Configuration.

Video

Watch Under the Hood of the Automated Configuration Tool for Citrix Virtual Apps and Desktops on YouTube.

Training

The Cloud Learning Center contains step-by-step video guides to building a service deployment, including the tasks described in this article. See Migrating Citrix Virtual Apps and Desktops to Citrix Cloud Learning Path.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Print

Managing printers in your environment is a multistage process:

1. Become familiar with printing concepts, if you are not already.
2. Plan your printing architecture. This includes analyzing your business needs, your existing printing infrastructure, how your users and applications interact with printing today, and which printing management model best applies to your environment.
3. Configure your printing environment by selecting a printer provisioning method and then creating policies to deploy your printing design. Update policies when new employees or servers are added.
4. Test a pilot printing configuration before deploying it to users.
5. Maintain your Citrix® printing environment by managing printer drivers and optimizing printing performance.
6. Troubleshoot issues that may arise.

For complete information about printing in a Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) environment, begin with Print. From that article, you can move on to:

- Printing configuration examples
- Best practices
- Printing policies and preferences
- Provison printers
- Maintain the printing environment

Install the Universal Print Server on your print servers

1. Ensure that each print server has Microsoft Virtual C++ Runtime 2017, 32-bit and 64-bit installed.
2. Navigate to the Citrix Universal Print Server download page and click **Download File**.
3. Run one of the following commands on each print server:
    - For a 32-bit operating system: **UpsServer_x86.msi**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For a 64-bit operating system: **UpsServer_x64.msi**.

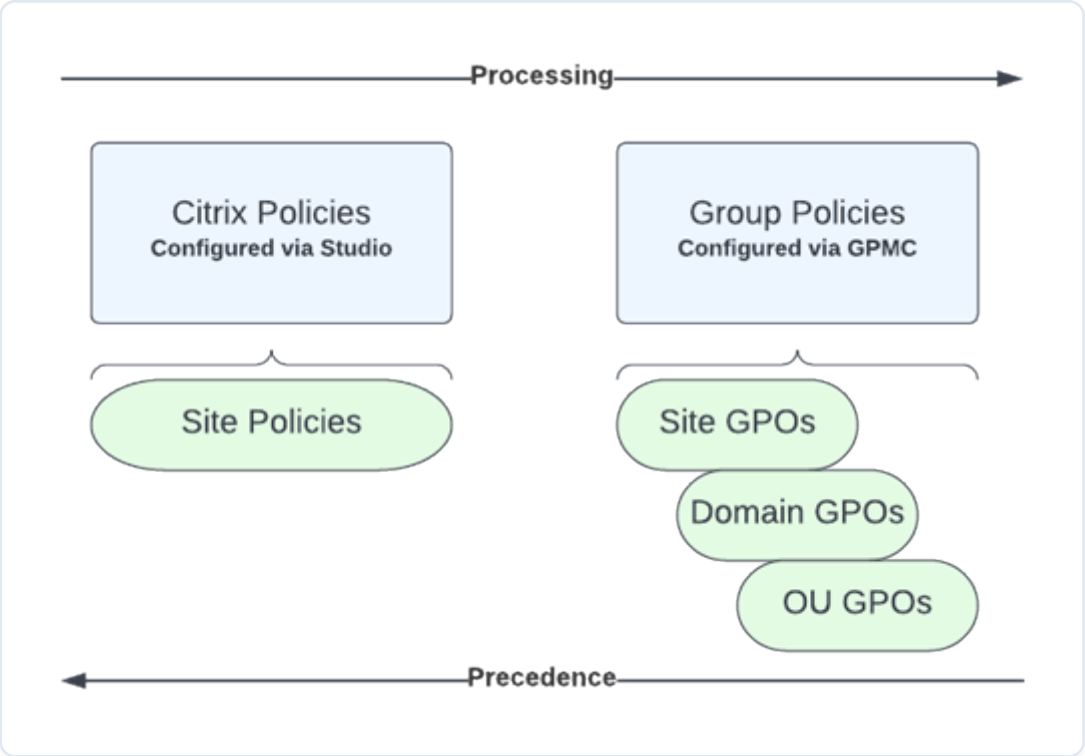
After you install the Universal Print Server, configure it using the guidance in Provision printers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policies

Policies are a collection of settings that define how sessions, bandwidth, and security are managed for a group of users, devices, or connection types.

You can apply policy settings to VDAs or to users. You can edit settings in Web Studio or in the Active Directory Group policy objects (GPOs). You can specify filters (object assignments) for policies. If you do not specifically assign policies to filters, settings are applied to all user sessions.



You can apply policies on different levels of the network. Policy settings placed at the Organizational Unit GPO level take the highest precedence on the network. Policies at the Domain GPO level override policies on the Site Group Policy Object level. The Site Group Policy Object level overrides any conflicting policies on both the Microsoft and Citrix Local Policies levels.

All Citrix Site Policies are created and managed in the Web Studio console and stored in the Site Database. Group Policies are created and managed by using the Microsoft Group Policy Management Console (GPMC) and stored in the Active Directory. Microsoft Local Policies are created in the Windows Operating System and are stored in the registry.

Web Studio uses a Modeling Wizard to help administrators compare configuration settings within templates and policies to help eliminate conflicting and redundant settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Settings are merged according to priority and their condition. Any disabled setting overrides a lower-ranked enabled setting. Unconfigured policy settings are ignored and do not override lower-ranked settings.

Web Studio policies can also have conflicts with group policies in the Active Directory, which might override each other depending on the situation.

All policies are processed in the following order:

1. From the Citrix Workspace™ app, the end user logs on to a VDA using domain credentials.
2. Citrix policies are processed for the end user and for the VDA
3. Policies are applied in the following order:
    a. Local policies
    b. Site policies
    c. Domain policies
    d. OU (Organizational unit) policies

NOTE:

- All policies might not be present at the four levels. For most of the customers, only site policies are used. Local policies require the user to log on to VDA to edit policies. Hence, these policies are almost never used.
- We do not support mixing Windows and Citrix policies in the same GPO.

Overview

Policies are a collection of settings that define how sessions, bandwidth, and security are managed for a group of users, devices, or connection types. Citrix® policies provide an efficient way to manage these aspects centrally. Each policy can include multiple settings and filters (object assignments) tailored to your environment.

Tools for managing policies

- Studio

  Policies that are created using Studio are stored in the DaaS control plane, and the updates are pushed to the VDA either of the following happens:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When that VDA registers with the DaaS control plane
- When a user launches a session

- Group Policy Management Console (GPMC)

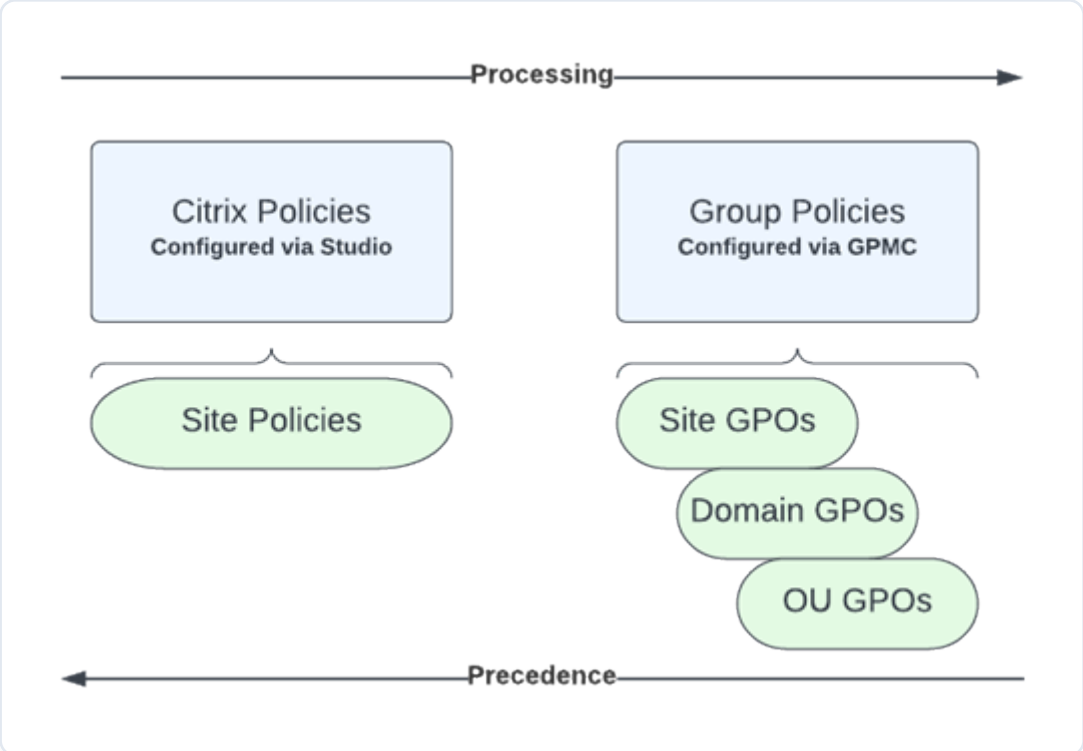
  If your network environment uses Active Directory and you have permission to manage group policy, you can use the GPMC to create and edit policies.

  In GPMC, you can configure Group Policy Objects (GPOs) with the settings and filters you need. These policies take priority over policies configured in Studio. For more information, see CTX238166.

Policy processing order

Group policy settings are processed in the following order:

1. Site-level GPO (stored in the DaaS control plane)
2. Domain-level GPOs
3. Organizational Units (OU) GPOs



If different settings are applied for the same policy in two GPOs, the policy settings processed last overwrite the settings processed earlier. This configuration means that policy settings take precedence in the following order:

1. OU GPOs (highest priority)

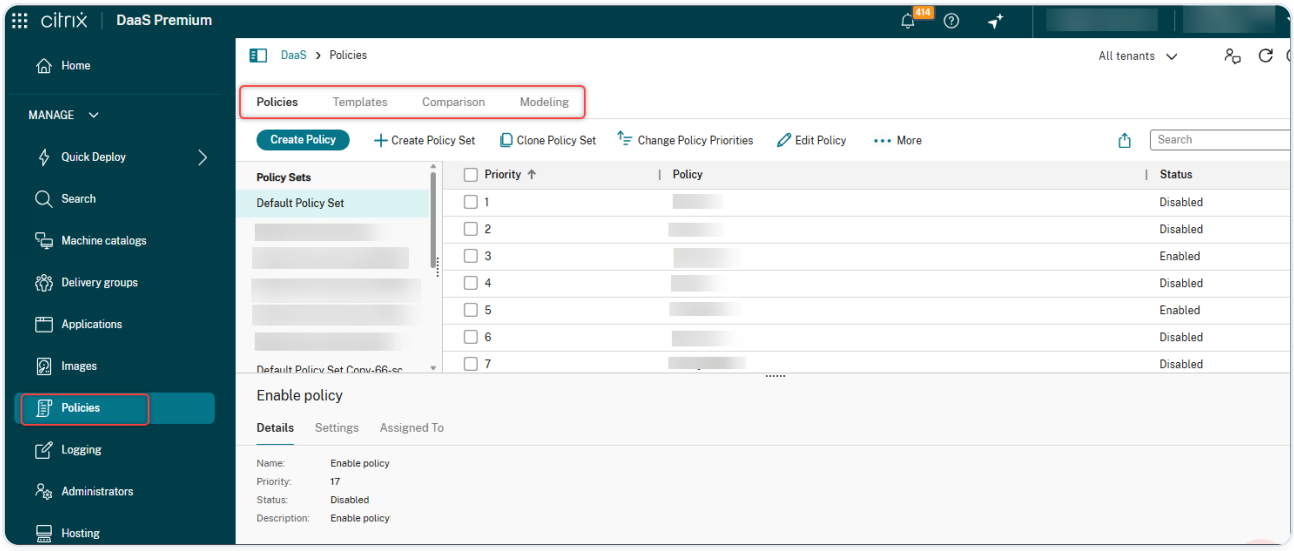
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Domain-level GPOs
3. Site-level GPOs (lowest priority)

If you're using multiple policies with conflicting settings, you can control precedence by assigning policy priorities. For more information, see Manage advanced policy scenarios.

Learn about the Studio > Policies interface

To access policies, settings, or templates, sign in to Studio and then select **Policies** in the left pane.



- The **Policies** tab lets you create and manage policy sets and policies. When you select a policy from a policy set, the following tabs appear:
  - **Overview** – Displays the policy name, priority, status, and description.
  - **Settings** – Lists all configured settings.
  - **Assigned To** – Shows assigned delivery groups. You can edit or remove assignments. Policies are applied based on the delivery group of the desktop running the session. For details, see Create policies.
- The **Templates** tab lets you create policy templates and manage Citrix-provided and custom templates. When you select a template, the following tabs appear:
  - **Description** – Explains the purpose of the template.
  - **Settings** – Lists the configured settings. For details, see Policy templates.
- The **Comparison** tab lets you compare settings in a policy or template with others. Use this feature to check for compliance or differences. For details, see Manage advanced policy scenarios.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **Modeling** tab Lets you simulate connection scenarios and view effective policy results. For details, see Manage advanced policy scenarios.

Policy configuration workflow

To configure Citrix policies using Studio, follow this workflow:

1. Create the policy.
   a. Configure policy settings.

      Add and configure the settings required for your environment.

   b. Assign the policy.

      Assign the policy to the appropriate machine and user objects.
2. Set policy priority.

   Arrange policies in priority order to determine which settings take precedence.
3. Verify the effective policy.

   Use the Policy Modeling wizard to confirm the applied settings.

Create templates

Templates provide a predefined starting point for creating policies. We offer built-in templates optimized for specific environments and network conditions. You can use these templates to:

- Create your own policies and templates to share across sites.
- Reference during comparisons across deployments. For example, “...when using the Citrix template X or Y...”.
- Communicate policy configurations with Citrix Support or trusted third parties by importing or exporting templates.

Built-in templates

The following built-in templates are available:

- **Very High Definition User Experience**. This template enforces default settings that maximize the user experience. Use this template in scenarios where multiple policies are processed in order of precedence.

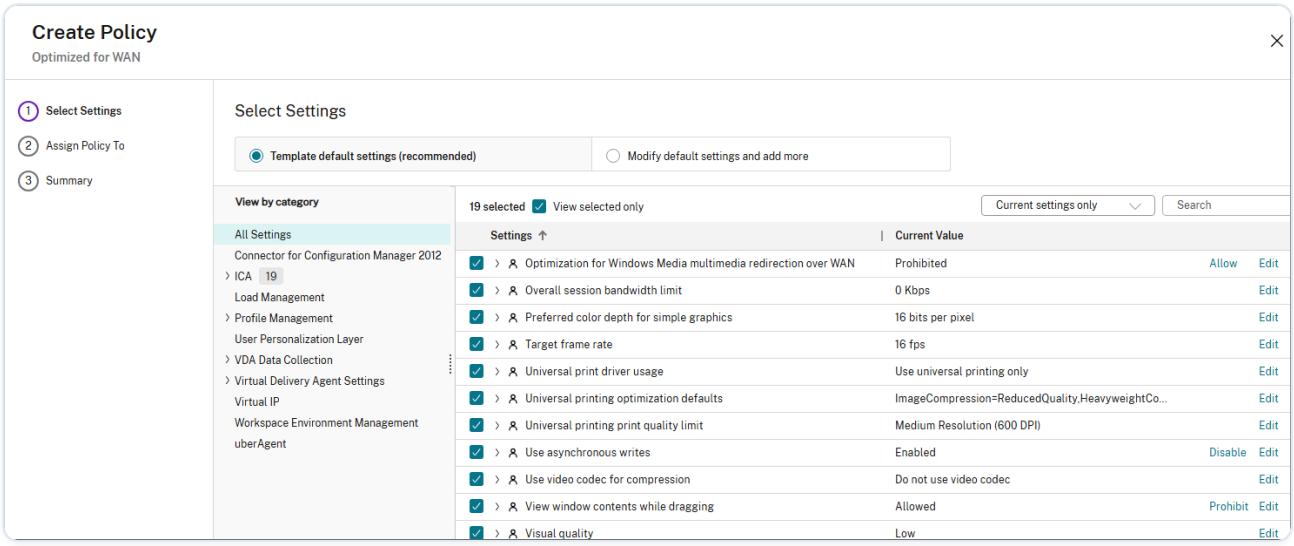
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **High Server Scalability**. Apply this template to economize on server resources. This template balances user experience and server scalability. It offers a good user experience while increasing the number of users that you can host on a single server. This template does not use a video codec for compression of graphics and prevents server-side multimedia rendering.
- **High Server Scalability-Legacy OS**. This High Server Scalability template applies only to VDAs running Windows Server 2008 R2 or Windows 7 and earlier. This template relies on the Legacy graphics mode, which is more efficient for those operating systems.
- **Optimized for NetScaler SD-WAN.** Apply this template for users working from branch offices with NetScaler SD-WAN for optimizing delivery of Citrix Virtual Desktops. (NetScaler SD-WAN is the new name for CloudBridge).
- **Optimized for WAN**. This template intends for task workers in branch offices who uses shared WAN or remote locations with low bandwidth connections. The workers access applications with graphically simple user interfaces and little multimedia content. This template trades off video playback experience and some server scalability for optimized bandwidth efficiency.
- **Optimized for WAN-Legacy OS**. This template applies only to VDAs running Windows Server 2008 R2 or Windows 7 and earlier. This template relies on the Legacy graphics mode, which is more efficient for those operating systems.
- **Security and Control**. Use this template in environments with low tolerance to risk, to minimize the features enabled by default in Citrix DaaS. This template includes settings that disable access to the following:
  - Printing
  - Clipboard
  - Peripheral devices
  - Drive mapping
  - Port redirection
  - Flash acceleration on user devices

  Applying this template might use more bandwidth and reduce user density per server.

While We recommends using the default settings in built-in templates, some settings, such as **Overall session bandwidth limit** in the **WAN templates**, are left unconfigured to allow administrators to make deployment-specific adjustments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Consider that you are working with a deployment (policy management and VDAs) earlier than XenApp and XenDesktop 7.6 FP3. Also, require High Server Scalability and Optimized for WAN templates. In this case, use the Legacy OS versions of these templates when they apply.

NOTE:

We create and updates built-in templates. You cannot modify or delete these templates.

Create templates

To create a template from a template:

1. In Studio, select **Policies** in the left pane.
2. Select the **Templates** tab and then select the template from which you create the template.
3. Select **Create Template** tab. The **Select Settings** screen appears.
4. Select and configure the policy settings to include in the template.
5. Click **Next**. The **Summary** screen appears.
6. Enter a name for the template.
7. Click **Finish**. The new template appears on the **Templates** tab

To create a template based on a policy:

1. In Studio, select **Policies** in the left pane.
2. On the **Policies** tab, select the policy from which you create the template.
3. Click **More** tab.
4. Select **Save as Template**. The **Select Settings** screen appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select and configure any new policy settings to include in the template.
6. Click **Next**. The **Summary** screen appears.
7. Enter a name and description for the template, and then click **Finish**.

Create policies

A policy defines two parts:

- A group of settings that define how sessions, bandwidth, and security are managed for a group of users, devices, or connection types.
- Users and machines to assign the policy to. Before creating a policy, decide which group of users or devices it affects. You might want to create a policy based on job function, connection type, device platform, or geographic location.

When you create a policy, you can base it on settings from a policy template and customize them as needed. You can also start from scratch and manually add the necessary settings. This section covers the following topics:

- How policies work
- Create policies from scratch
- Create policies from templates

TIP

If a policy exists for a group, consider editing it rather than creating one. Avoid creating policies solely to enable a specific setting or exclude specific users.

How policies work

When a user logs on, all policies that match the assignments for the connection are identified. Those policies are ranked by priority and multiple instances of any setting are compared. For each setting, the value from the highest-priority policy is applied. If a higher-priority policy disables a setting, that setting overrides any lower-priority policy where it's enabled. Settings that aren't configured are ignored.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

If you're configuring both Active Directory and Citrix policies using the Group Policy Management Console, assignments and settings might not apply as expected. For more information, see CTX127461.

The Unfiltered policy

We provide a default policy called **Unfiltered**.

- When you manage Citrix® policies in Web Studio, settings in the Unfiltered policy apply to all servers, desktops, and connections in the Site.
- For the settings to apply, the Site and connections must fall within the scope of the GPO containing the policy.

  Example: A GPO named **Sales-US** is linked to the **Sales** OU and includes all US sales team members. This GPO is configured with an **Unfiltered** policy with several user settings. When a sales manager logs on, the **Unfiltered** policy settings are applied because the user is in the **Sales-US** GPO.

Assignment modes

Assignment mode controls whether a policy applies based on how the connection criteria match.

- **Allow** (default): Applies the policy only if the connection matches the assignment criteria.
- **Deny**: Applies the policy if the connection doesn't match the criteria.

Example 1: Same assignment type, different modes

Policy 1 includes:

- Assignment A: Sales group, mode = Allow
- Assignment B: Sales manager's account, mode = Deny

Although the user is in the Sales group, the Deny assignment takes precedence. The policy doesn't apply when the sales manager logs on.

Example 2: Different assignment types, same mode

Policy 2 includes:

- Assignment C: Sales group (User), mode = Allow

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Assignment D: Corporate IP range (Client IP), mode = Allow

The policy applies only when both assignments are satisfied. If the sales manager logs on from the office, both conditions are met, and the policy applies.

Policy 3 includes:

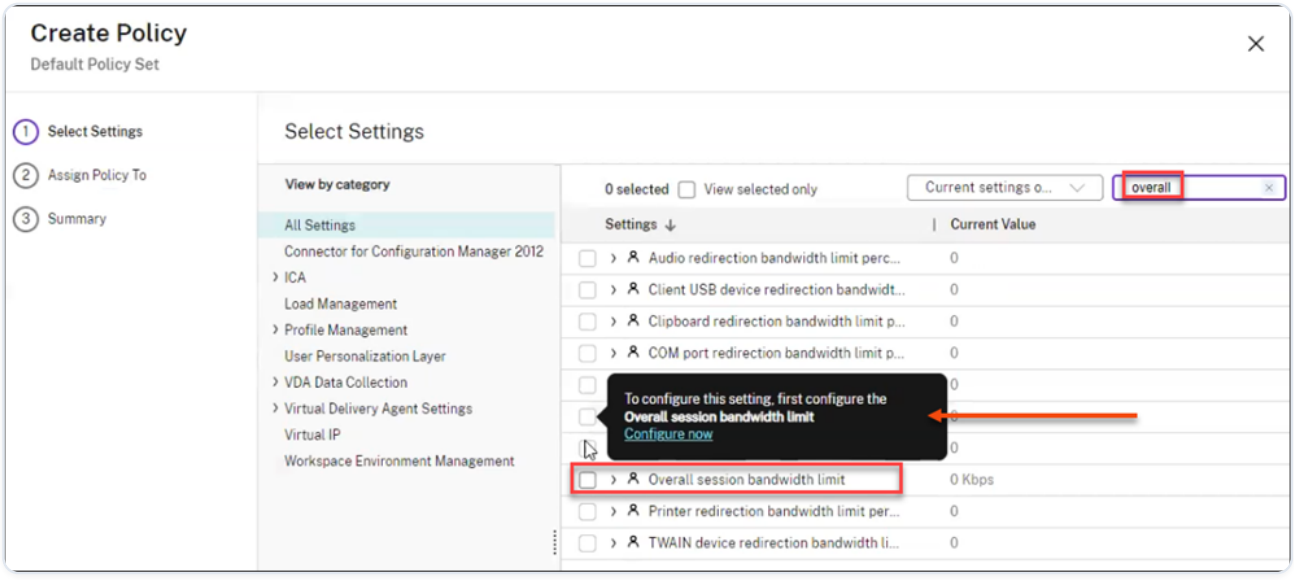
- Assignment E: Sales group (User), mode = Allow
- Assignment F: NetScaler Gateway connection (Access Control), mode = Allow

If the sales manager logs on from the office (not through NetScaler), Assignment F isn't satisfied, so the policy doesn't apply.

Policy settings: Parent-child relationships

Some policy settings depend on parent settings. For example, you must configure **Overall session bandwidth limit** before its child settings become available.

When configuring policies in Web Studio, hover over a child setting to see which parent must be configured first. If a parent is disabled, related child settings are automatically disabled.



The following table lists parent settings and their corresponding child settings:

PARENT POLICY	DEPENDENT CHILD POLICIES
Overall session bandwidth limit	Audio redirection bandwidth limit percent
	Clipboard redirection bandwidth limit percent
	COM port redirection bandwidth limit percent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARENT POLICY	DEPENDENT CHILD POLICIES
	File redirection bandwidth limit percent
	HDX™ MediaStream Multimedia Acceleration bandwidth limit percent
	LPT port redirection bandwidth limit percent
	Printer redirection bandwidth limit percent
	Client USB device redirection bandwidth limit percent
	TWAIN device redirection bandwidth limit percent
Allow bidirectional content redirection	Allowed URLs to be redirected to Client
	Allowed URLs to be redirected to VDA
CPU usage	CPU usage excluded process priority
Legacy graphics mode	Progressive compression level
Enable session watermark	Watermark custom text
	Session watermark style
	Watermark transparency
HDX adaptive transport	Loss tolerant mode for audio

Policy setting states

Some policy settings can have one of the following states:

- **Allowed** or **Prohibited**: Allows or prevents the action controlled by the setting. Sometimes users are allowed or prevented from managing the setting's action in a session. For example, if the menu animation is set to Allowed, users can control it within their session.
- **Enabled** or **Disabled**: turns the setting on or off. If a setting is disabled in a higher-priority policy, it's not applied—even if enabled in a lower-priority policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

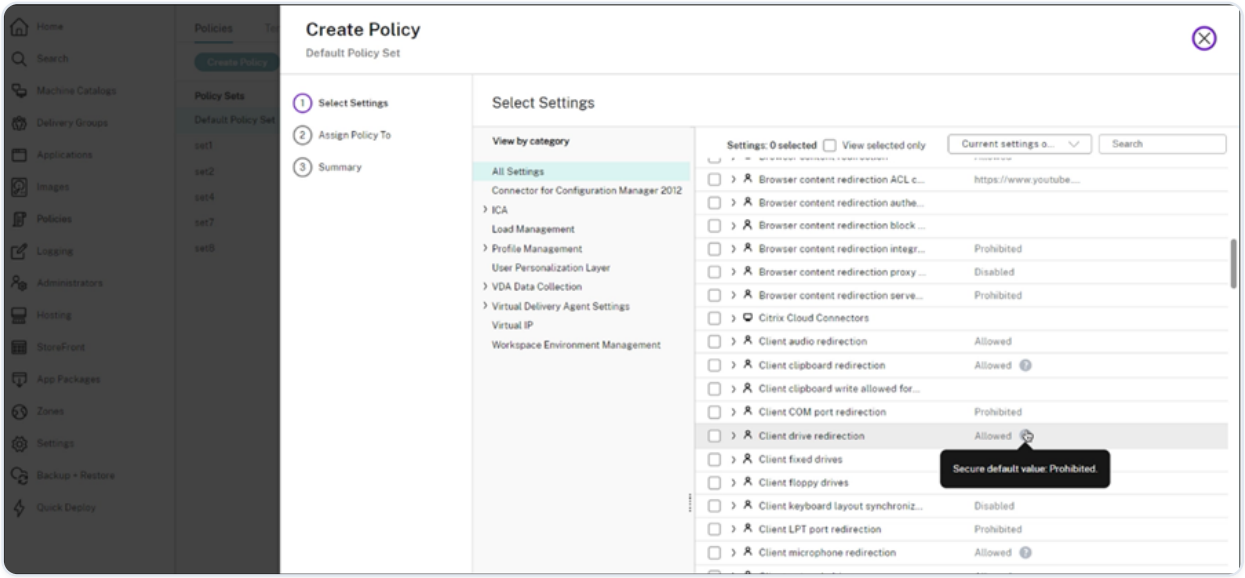
Secure default settings

If the secure default setting is enabled during VDA installation, the priority of the policy settings is as follows:

1. Customized setting
2. Secure default setting
3. Default setting

To view the secure default value:

1. In Web Studio, click **Policies** in the left pane.
2. On the **Policies** tab, click **Create Policy**.
3. In the **Select Settings** table, when you hover-over the settings that have **Allowed** as their current value, the **Secure default value: Prohibited** is shown.



Policy setting effectiveness

Some settings must be used and enabled together. For example, to allow users to access network drives on their local device:

- **Client drive redirection** must be enabled
- **Client network drives** must also be included

If **Client drive redirection** is disabled, users can't access network drives even if **Client network drives** is enabled.

In general, changes to machine-related settings take effect when the VDA restarts or a user logs on. Changes to user-related settings apply at the next logon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When adding a setting to a policy, you can select Use the default value to prevent changes. This option disables manual configuration and applies the default value only, regardless of previously entered values.

Best practices

- Assign policies to groups rather than individual users. If you assign policies to groups, assignments are updated automatically when you add or remove users from the group.
- Disable unused policies. Policies with no settings added incur unnecessary processing overhead.

Create policies from scratch

To create a policy:

1. In Web Studio, click **Policies** in the left pane.
2. On the **Policies** tab, click **Create Policy**.
3. On the **Select Settings** page, select and configure settings and then click **Next**.
4. On the **Assign Policy to** page, select the policy set where this policy resides, and then select the objects to assign the policy to. Click **Next**.
5. On the **Summary** page, complete the following settings:
    a. Enter a name and description for the policy.
    b. To enable the policy, select **Enable policy**.
6. Click **Finish**.

Step 1: Select and configure policy settings

Policy settings are grouped by function. For example, settings related to Profile Management are under the **Profile Management** category.

There are two types of settings:

- **Computer settings**: Apply to machines and take effect when the virtual desktop starts (even if no user is logged on). They define virtual desktop behaviors.
- **User settings**: Apply when a user connects or reconnects. They define the user experience.

To select and configure a setting:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. On the **Select Settings** page, to view settings by VDA versions, select one of the following options from the drop-down list option on the upper-right side:
   - **All settings**: View all settings for all VDA versions
   - **Current settings only**: View settings only for the current VDA versions
   - **Legacy settings only**: View settings only for deprecated VDA versions
2. To search for a setting, enter the complete or partial name of the setting in the search box.
3. Select a setting. Click **Enable** to turn it on or **Edit** to specify a value.
4. Repeat step 3 to select and configure more settings for the policy.

> **NOTE:**
>
> Policy settings can be Enabled, Disabled, or Not configured. By default, policy settings aren't configured, which means they aren't added to a policy. Settings are applied only when they're added to a policy.

Step 2: Specify policy assignments

Policy assignments define which users and machines a policy applies to. For information about how assignments affect policy behavior, see How policies work.

To specify policy assignments:

1. On the **Assign Policy To** page, select **Filtered users and computers**.
2. Select the users or computers by specifying assignments (also known as *filters*). Refer to the following table for available assignment types.

> **NOTE:**
>
> - If you do not specify any assignments or disable them, the policy applies to **all** connections.
> - Policy *assignments* are also known as policy *filters*. For more information, see Create, modify, or delete a filter for a policy and How do filters get applied?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ASSIGNMENT TYPE	DESCRIPTION
Access Control	Access control conditions through which a client is connecting: • **Connection type**: Whether to apply the policy to connections made with or without NetScaler® Gateway. *NetScaler Gateway farm name* - Name of the NetScaler Gateway virtual server. *Access condition* - Name of the end point analysis policy or session policy to use. • **NetScaler Gateway farm name**: Name of the NetScaler Gateway virtual server. *Access condition* - Name of the end point analysis policy or session policy to use. • **Access condition**: Name of the end point analysis policy or session policy to use.
Citrix SD-WAN™	Whether a user session is launched through Citrix SD-WAN. **Note:** You can add only one Citrix SD-WAN assignment to a policy.
Client IP Address	IP address of the user device used to connect to the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ASSIGNMENT TYPE	DESCRIPTION
	session: IPv4 examples: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6 examples: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Client Name	Name of the user device. Exact match: ClientABCName. Using wildcard: Client*Name.
Client Platform	OS type of the user device used to connect the session, such as Windows, Linux, iOS, Android, or HTML5. Required VDA version: 2503 or later.
Delivery Group	Delivery Group membership.
Delivery Group type	Type of desktop or application: private desktop, shared desktop, private application, or shared application.
Organizational Unit (OU)	Organizational unit.
Tag	Tags. **Note:** Apply this policy to all tagged machines. Application tags aren't included.
User or Group	User or group name. The supported identity types for users and groups include Active Directory, Microsoft Entra ID, Okta, and Google Cloud. Required VDA version: 2507 or later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create policies from templates

You can create a policy based on a Citrix-provided or custom template. The resulting policy is independent of the original template.

To create a policy from a template:

1. In Web Studio, select **Policies** in the left pane.
2. Select the **Templates** tab, and then select the template you want to use.
3. Click **Create Policy from Template** in the action bar. The **Create Policy** page appears, showing all settings preconfigured in the selected template.
4. Modify the settings and add more settings if needed, and then click **Next**.
5. On the **Assign Policy to** page, select the policy set where this policy resides, and then select the objects to assign the policy to. Click **Next**.
6. On the **Summary** page, enter a name and description for the policy.
7. Click **Finish**. The new policy appears in the specified policy set on the **Policies** tab.

Where to go next

- Prioritize policies
- Simulate and evaluate policies

Create policy sets

Policy sets are objects in Citrix DaaS™ that aggregates policies to allow for simplified, role-based access, and easy management. Once created, scopes and delivery groups are assigned to policy sets so that only authorized administrators can manage the policies that apply to their relevant users and machines.

Policy sets help you manage Citrix® policies more efficiently by organizing them into logical groups. When you assign a policy set to a delivery group, the delivery group uses only the policies in that set.

This section explains how policy sets behave, how to create and assign them, and how they interact with scopes and filters.

Benefits

Policy sets offer several key benefits:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Role-based access control for distributed administrator teams
- Simplified mergers, acquisitions, and consolidations
- Limited fault domain
- Multitenant support for policies

The following table compares how policies work with and without policy sets:

WITHOUT POLICY SETS	WITH POLICY SETS
All policies, settings, filters (assignments), and priorities are managed in one central location.	Each policy set has its own settings, filters (assignments), and priorities.
If you manage one policy, you must manage every policy.	Full administrators can delegate to lower-level admins the ability to manage a particular policy set on an individual basis.
Policies in large and distributed environments become complex and difficult to manage.	Policies in large and distributed environments can be divided and managed easily.

How it works

Policy sets are assigned to delivery groups and scoped to specific administrators. Policies within a set continue to use filters (assignments) to determine which users or machines they apply to.

Key behaviors:

- Policy sets are assigned to delivery groups
  - A delivery group can use only one policy set at a time.
  - A policy set can be assigned to multiple delivery groups.
  - If a delivery group doesn't have a policy set assigned, it uses **Default Policy Set**.
- Filters on policies still apply, regardless of whether the policy is in a set.
- A policy set can have one or multiple scopes.
  - A scope represents a collection of objects (for example, connections, catalogs, delivery groups, and application groups) that administrators can manage.
  - As administrators, you can define the scope of the policy set so that only authorized administrators can view or edit it. You can set scopes during policy set creation or when editing the set later.

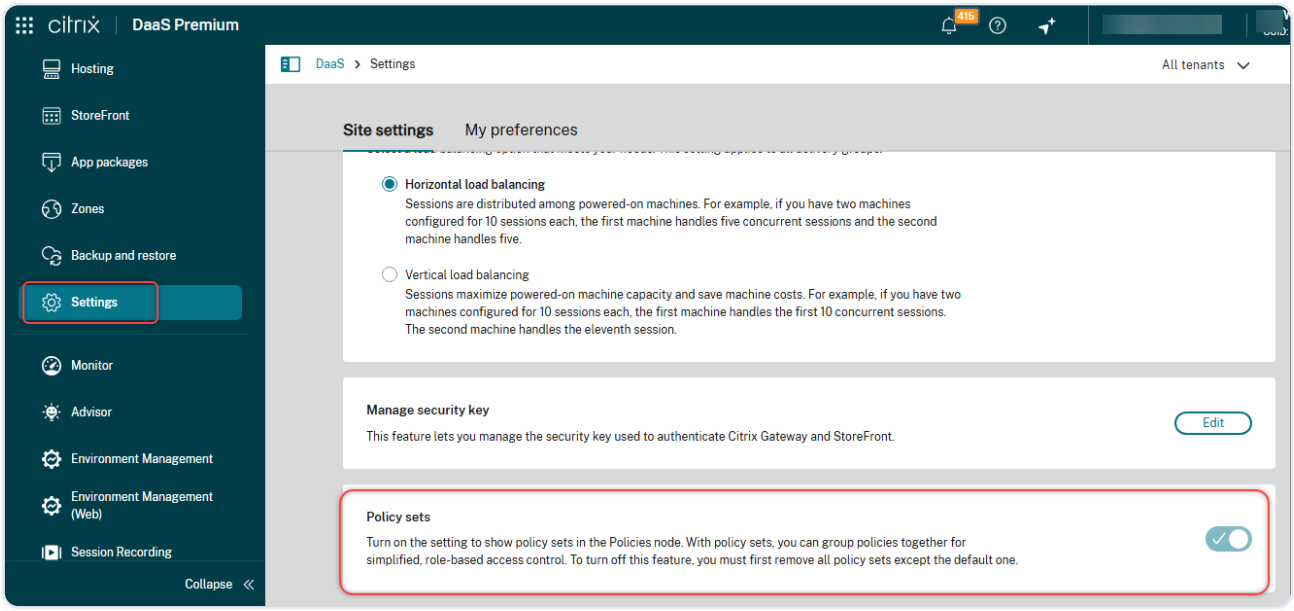
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **Default Policy Set** has **Bypass scope control for this resource** selected by default. This setting ensures that the policy set remains visible to all administrators. To apply scope control, edit the policy set, clear the **Bypass scope control for this resource** checkbox, and then select the desired scopes.

Policy filters and assignments work the same way as they do without policy sets. For more information, see How do filters get applied.

Enable policy sets

In Studio, go to **Settings > Site settings** and turn on the **Policy sets** setting.



NOTE:

- You must enable policy sets before creating a policy set.
- When you enable policy sets, all existing policies are grouped into **Default Policy Set**. This set is automatically assigned to all delivery groups unless you assign a different set. After a new policy set is assigned to a delivery group, that group stops using the default policy set.

Create policy sets

You can create policy sets to mirror logical divisions in your administrator team and company. For example, you can create a policy set for each geographic region, business-unit, or for specific use case.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can create policy sets in two ways:

- Create policy sets from scratch
- Create a policy set by copying an existing one

Alternatively, you can use the Citrix DaaS REST APIs to create and manage policy sets. For more information, see How to create a policy set in Citrix DaaS.

Create policy sets from scratch

1. In Studio, select the **Policies** node in the left pane.
2. Click the **Policies** tab.
3. Select **Create Policy Set**.
4. Click the **Name and Description** tab, and enter the name and description for the policy set.
5. Click the **Assignments** tab, and select one or more delivery groups.
6. Click the **Scopes** tab, and select the scopes that define the objects that the policy set can apply to.
7. Click **Create** to finish.

Clone policy sets

1. In Studio, select the **Policies** node in the left pane.
2. Click the **Policies** tab.
3. Select **Clone Policy Set**.
4. Update the name of the policy set.
5. Update or create assignments for the policy set and click **Next**.
6. Select or clear policies to include in the cloned policy set.
7. Update the scope of the policy.
8. Click **Create**.

Prioritize policies

When multiple policies apply to a connection, Citrix DaaS™ evaluates them in priority order. A lower number means a higher priority (1 is the highest). When conflicting settings exist across policies, the setting from the highest-priority policy takes effect.

You can change policy priority using Web Studio or PowerShell.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change policy priority using Web Studio

1. In **Web Studio**, select **Policies** in the left pane.
2. On the **Policies** tab, select **Change Policy Priorities** from the action bar.
3. On the **Change Policy Priorities** page, reorder policies using any of the following methods:
   - Drag a policy to a desired position.
   - Click the **Up** or **Down** arrow icon to move it one position.
   - Click the **Top** or **Bottom** arrow icon to move it to the first or last position.
   - Click the **Edit** icon, enter a priority number, and then click **Save**.
4. Click **Save** to apply changes.

Manage policy assignment exceptions

When you assign policies to groups of users, user devices, or machines using filters, some members of the group might need different settings. You can handle these cases without creating entirely separate policies for each individual.

You can make exceptions for certain users or machines within a group by:

- Creating a separate policy only for those group members and giving it higher priority
- Using the *Deny* mode for an assignment added to the policy

Use Deny mode for exceptions

An assignment with the mode set to *Deny* means that the policy applies to connections that don't match the assignment criteria. For example, a policy includes the following assignments:

- *Assignment A*: Client IP address assignment range `208.77.88.*`, mode = *Allow*.
- *Assignment B*: Specific user account, mode = *Deny*.

This policy applies to users connecting from the specified IP range, **except** the user defined in *Assignment B*.

NOTE:

In the **Assign Policy** step, if you clear the **Enable** checkbox, the assignment is disabled. If a policy has no enabled assignments, it applies to all objects in the site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related content

- Prioritize policies
- Simulate and evaluate policies

Simulate and evaluate policies

Use the comparison and Policy Modeling tools in Web Studio to verify your configurations, test policy behavior, and evaluate which settings apply before deploying them.

NOTE:

- The **Modeling** tab is available only if enabled by customer request.
- Only enabled policies with filters are modeled. Disabled policies are never applied; enabled policies without filters are always applied.

Compare policies and templates

Use the comparison feature in Web Studio to view the differences between policies, templates, or default settings. This helps you verify configuration consistency, maintain compliance with best practices, and troubleshoot unexpected behavior.

You can:

- Compare the settings of a policy or template with another
- Compare settings against default values
- Identify conflicting or missing configurations across policies

To compare policies and templates:

1. In Web Studio, select **Policies** in the left pane.
2. Click the **Comparison** tab and then click **Select**.
3. Choose the policies or templates to compare.
4. (Optional) Select **Compare to default settings** to include defaults.
5. Click **Compare**. Settings appear in columns.
    - To see all settings, select **Show All Settings**.
    - To return to the default view, select **Show Common Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Run the Policy Modeling wizard

1. In Web Studio, select **Policies**.
2. Select the **Modeling** tab.
3. Select **Policy Modeling** in the action bar.
4. Read the **Introduction** page and click **Next**.
5. Select users or computers. You can also browse for containers or specific users or computers. Click **Next**.
6. Choose your filter evidence. Optionally, refine the simulation by specifying details such as **Delivery group**, **Tags**, and **Client IP address**. Click **Next**.
7. Review the summary and click **Run**.

View and manage modeling results

After the wizard runs, it generates a report you can review, act on, and export.

Review the report

- Use the drop-down menu to view **All settings**, **Computer settings**, or **User settings**.
- Search for specific settings.
- Click a setting to see why it was or was not applied.
- Export results in JSON or HTML format.

Manage the report

The following options are available in the action bar after a simulation runs:

OPTION	DESCRIPTION
View Modeling Report	Review or export the results.
Rerun Policy Modeling	Run again using the same criteria.
Delete Modeling Report	Remove the current report.

Evaluate policy application using Resultant Set of Policy

If a connection does not behave as expected, conflicting policies might be the cause. Higher-priority policies can override others. Use Resultant Set of Policy (RSoP) to evaluate which settings apply to a given connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Two RSoP methods are available:

- **Citrix Group Policy Modeling Wizard**

  Simulate a connection scenario by specifying users and assignment conditions.

- **Group Policy Results**

  Generate a report of Citrix policies applied to a user and Virtual Delivery Agent (VDA).

NOTE:

Site policy settings created in **Web Studio** are not included in the Resultant Set of Policy when you run the Citrix Group Policy Modeling wizard from the Group Policy Management Console (GPMC). For the most comprehensive results, start the Policy Modeling wizard from **Web Studio**, unless you create policies using only the GPMC.

Troubleshoot policy issues

Users, IP addresses, and other assigned objects can have multiple policies applying simultaneously, which can lead to unexpected behavior.

If you run the Policy Modeling wizard and no policies apply to user connections, it might be because:

- No policies have assignments that match the evaluation criteria.
- Policies that match the assignment have no settings configured.
- Policies that match the assignment are disabled.

To resolve these issues:

- Enable the relevant policies.
- Configure at least one setting for each policy.

NOTE:

In double-hop scenarios (for example, a single-session OS VDA connecting to a multi-session OS VDA) Citrix policies treat the single-session OS VDA as the user device. Images cached for the second hop apply to the first-hop machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View applied policies in Director

Non-administrators can use **Director** to view the policies that apply to a user session. This is useful for verifying which policy settings are in effect without requiring access to Web Studio.

Policy settings reference

The policy settings for Citrix DaaS™ are the same as those for Citrix Virtual Apps and Desktops™. For more information, see Policy settings reference in the Citrix Virtual Apps and Desktops documentation.

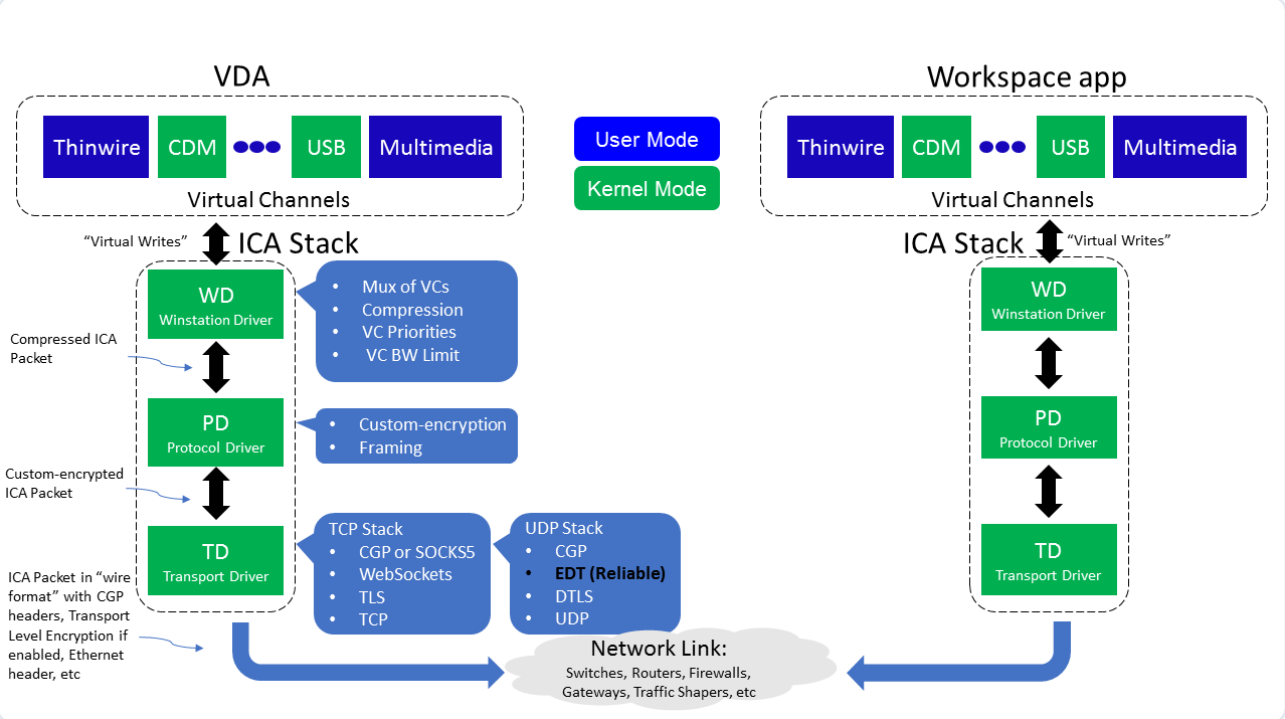
© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX™ overview

WARNING:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Citrix HDX represents a broad set of technologies that deliver a high-definition experience to users of centralized applications and desktops, on any device and over any network.



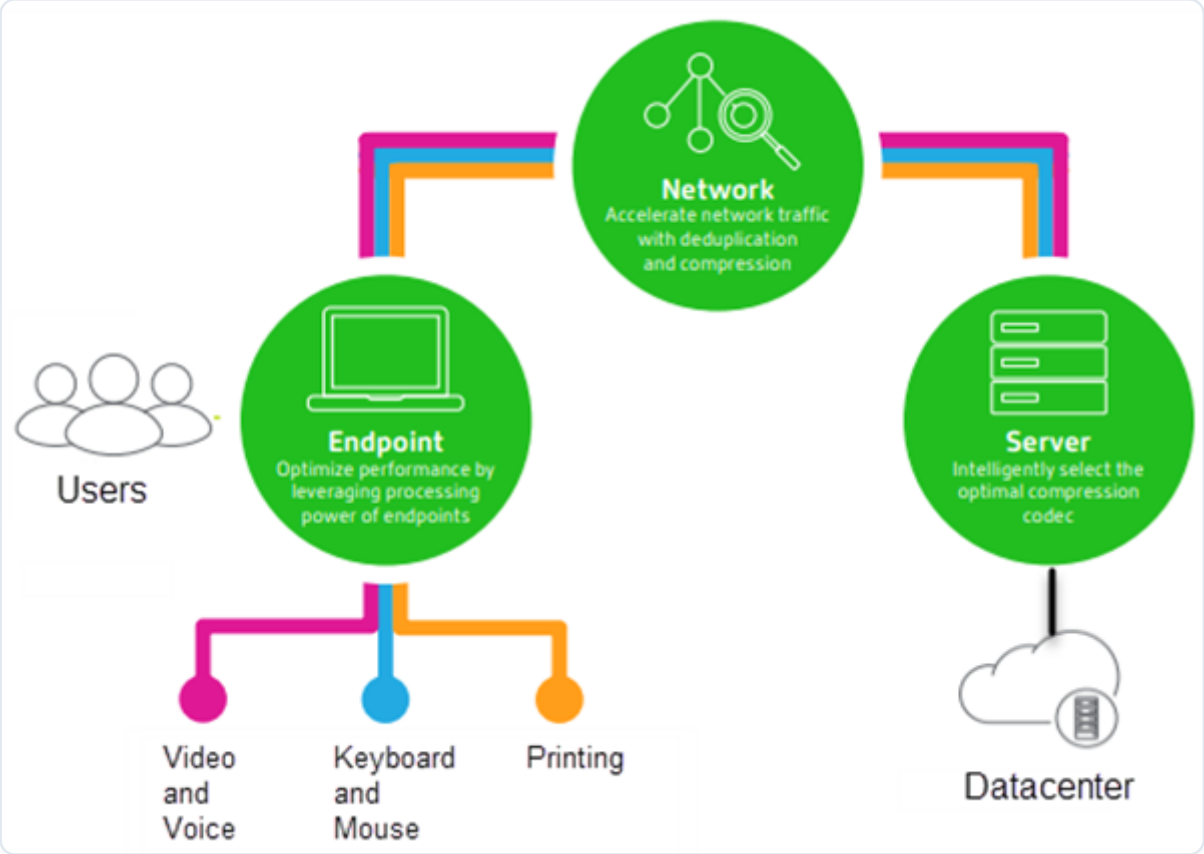
HDX is designed around three technical principles:

- Intelligent redirection
- Adaptive compression
- Data de-duplication

Applied in different combinations, they optimize the IT and user experience, decrease bandwidth consumption, and increase user density per hosting server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Intelligent redirection** - Intelligent redirection examines screen activity, application commands, endpoint device, and network and server capabilities to instantly determine how and where to render an application or desktop activity. Rendering can occur on either the endpoint device or hosting server.
- **Adaptive compression** - Adaptive compression allows rich multimedia displays to be delivered on thin network connections. HDX first evaluates several variables, such as the type of input, device, and display (text, video, voice, and multimedia). It chooses the optimal compression codec and the best proportion of CPU and GPU usage. It then intelligently adapts based on each unique user and basis. This intelligent adaptation is per user, or even per session.



- **Data de-duplication** - De-duplication of network traffic reduces the aggregate data sent between client and server. It does so by taking advantage of repeated patterns in commonly accessed data such as bitmap graphics, documents, print jobs, and streamed media. Caching these patterns allows only the changes to be transmitted across the network, eliminating duplicate traffic. HDX also supports multicasting of multimedia streams, where a single transmission from the source is viewed by multiple subscribers at one location, rather than a one-to-one connection for each user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

At the device

HDX uses the computing capacity of user devices to enhance and optimize the user experience. HDX technology ensures that users receive a smooth, seamless experience with multimedia content in their virtual desktops or applications. Session reconnect enables users to pause virtual desktops and applications and resume working from a different device at the point where they left off.

On the network

HDX incorporates advanced optimization and acceleration capabilities to deliver the best performance over any network, including low-bandwidth and high-latency WAN connections.

HDX features adapt to changes in the environment. The features balance performance and bandwidth. They apply the best technologies for each user scenario, whether the desktop or application is accessed locally on the corporate network or remotely from outside the corporate firewall.

In the data center

HDX uses the processing power and scalability of servers to deliver advanced graphical performance, regardless of the client device capabilities.

HDX channel monitoring provided by Citrix Director displays the status of connected HDX channels on user devices.

HDX Insight

HDX Insight is the integration of NetScaler® Network Inspector and Performance Manager with Director. It captures data about ICA traffic and provides a dashboard view of real time and historical details. This data includes client-side and server-side ICA session latency, bandwidth use of ICA channels, and the ICA round-trip time value of each session.

You can enable NetScaler to use the HDX Insight virtual channel to move all the required data points in an uncompressed format. If you disable this feature, the NetScaler device decrypts and decompresses the ICA® traffic spread across various virtual channels. Using the single virtual channel lessens complexity, enhances scalability, and is more cost effective.

Minimum requirements:

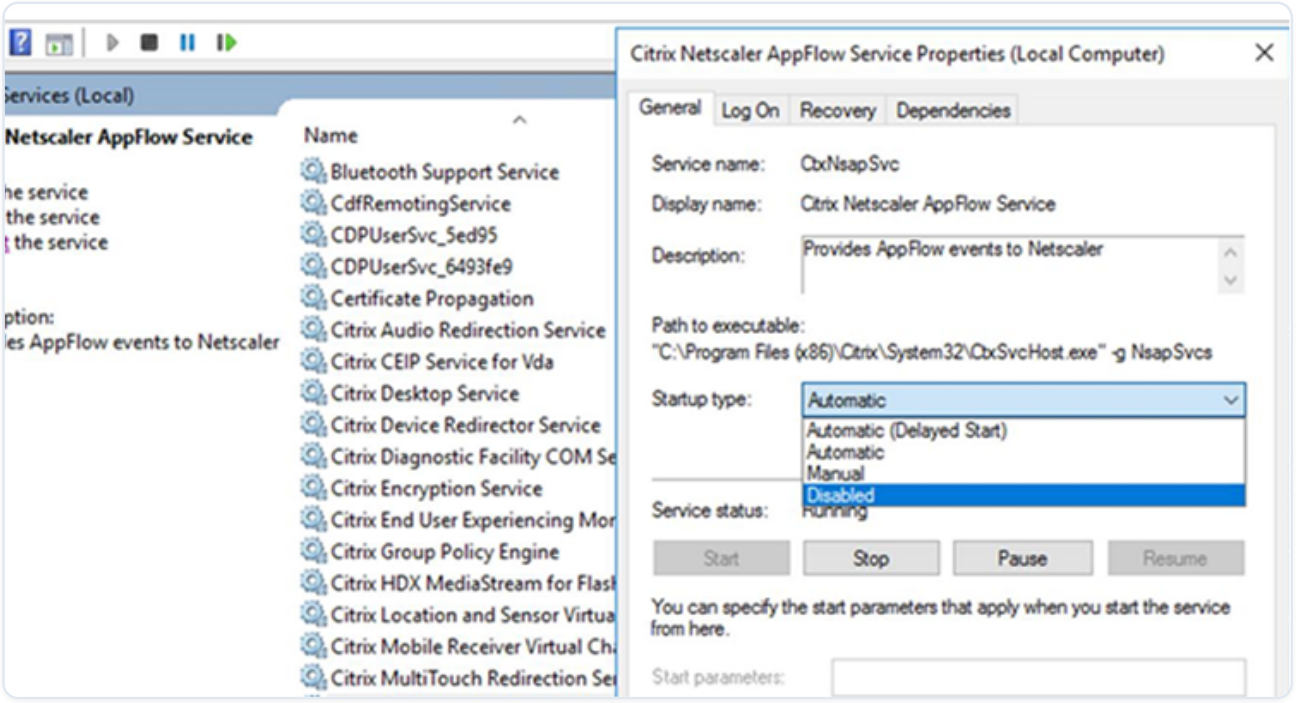
- Citrix Virtual Apps and Desktops™ 7 v1808

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- XenApp and XenDesktop 7.17
- NetScaler version 12.0 Build 57.x
- Citrix Workspace™ app for Windows 1808
- Citrix Receiver for Windows 4.10
- Citrix Workspace app for Mac 1808
- Citrix Receiver for Mac 12.8

Enable or disable HDX Insight virtual channel

To disable this feature, set the Citrix NetScaler Application Flow service properties to Disabled. To enable, set the service to Automatic. In either case, we recommend that you restart the server machine after changing these properties. By default, this service is enabled (Automatic).



Experience HDX capabilities from your virtual desktop

- To see how browser content redirection, one of four HDX multimedia redirection technologies, accelerates delivery of HTML5 and WebRTC multimedia content:

  a. Download the Chrome browser extension and install it on the virtual desktop.

  b. To experience how browser content redirection accelerates the delivery of multimedia content to virtual desktops, view a video on your desktop from a website containing HTML5 videos, such as YouTube. Users don't know when browser content redirection is running. To see whether browser content redirection is being used, drag the browser window quickly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You'll see a delay or out of frame between the viewport and the user interface. You can also right-click on the webpage and look for **About HDX Browser Redirection** in the menu.

- To see how HDX delivers high definition audio:

  a. Configure your Citrix client for maximum audio quality; see the Citrix Workspace app documentation for details.

  b. Play music files by using a digital audio player (such as iTunes) on your desktop.

HDX provides a superior graphics and video experience for most users by default, and configuration isn't required. Citrix policy settings that provide the best experience for most use cases are enabled by default.

- HDX automatically selects the best delivery method based on the client, platform, application, and network bandwidth, and then self-tunes based on changing conditions.
- HDX optimizes the performance of 2D and 3D graphics and video.
- HDX enables user devices to stream multimedia files directly from the source provider on the internet or intranet, rather than through the host server. If the requirements for this client-side content fetching are not met, media delivery falls back to server-side content fetching and multimedia redirection. Usually, adjustments to the multimedia redirection feature policies aren't needed.
- HDX delivers rich server-rendered video content to virtual desktops when multimedia redirection is not available: View a video on a website containing high definition videos, such as `<http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>`.

Good to know:

- For support and requirements information for HDX features, see the System requirements article. Except where otherwise noted, HDX features are available for supported Windows Multi-session OS and Windows Single-session OS machines, plus Remote PC Access desktops.
- This content describes how to optimize the user experience, improve server scalability, or reduce bandwidth requirements. For information about using Citrix policies and policy settings, see the Citrix policies documentation for this release.
- For instructions that include editing the registry, use caution: editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auto client reconnect and session reliability

When accessing hosted applications or desktops, network interruption might occur. To experience a smoother reconnection, we offer auto client reconnect and session reliability. In a default configuration, session reliability starts and then auto client reconnect follows.

Auto client reconnect:

Auto client reconnect relaunches the client engine to reconnect to a disconnected session. Auto client reconnect closes (or disconnects) the user session after the time specified in the setting. If auto client reconnect is in progress, the system sends application and desktops network interruption notification to the user as follows:

- **Desktops.** The session window is grayed out and a countdown timer shows the time until the reconnections occur.
- **Applications.** The session window closes and a dialog appears to the user containing a countdown timer showing the time until the reconnections are attempted.

During auto client reconnect, sessions relaunch expecting network connectivity. User cannot interact with sessions while auto client reconnect is in progress.

On reconnection, the disconnected sessions reconnect using saved connection information. The user can interact with the applications and desktops normally.

Default auto client reconnect settings:

- Auto client reconnect timeout: 120 seconds
- Auto client reconnect: Enabled
- Auto client reconnect authentication: Disabled
- Auto client reconnect Logging: Disabled

For more information, see Auto client reconnect policy settings.

Session reliability:

Session reliability reconnects ICA sessions seamlessly across network interruptions. Session reliability closes (or disconnects) the user session after the time specified in the setting. After the session reliability timeout, the auto client reconnect settings take effect, attempting to reconnect the user to the disconnected session. When session reliability is in progress, application and desktops network interruption notification are sent to the user as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Desktops.** The session window becomes translucent and a countdown timer shows the time until the reconnections occur.
- **Applications.** The window becomes translucent along with connection interrupted pop ups from the notification area.

While session reliability is active, the user cannot interact with the ICA sessions. However, user actions like keystrokes are buffered for few seconds immediately after the network interruption and retransmitted when the network is available.

On reconnection, the client and the server resume at the same point where they were in their exchange of protocol. The session windows lose translucency and appropriate notification area pop ups are shown for applications.

Default session reliability settings

- Session reliability timeout: 180 seconds
- Reconnection UI opacity level: 80%
- Session reliability connection: Enabled
- Session reliability port number: 2598

For more information, see Session reliability policy settings.

NetScaler with auto client reconnect and session reliability:

If Multistream and Multiport policies are enabled on the server and any or all these conditions are true, auto client reconnect does not work:

- Session reliability is disabled on NetScaler Gateway.
- A failover occurs on the NetScaler appliance.
- NetScaler SD-WAN is used with NetScaler Gateway.

HDX adaptive throughput

HDX adaptive throughput intelligently fine-tunes the peak throughput of the ICA session by adjusting output buffers. The number of output buffers is initially set at a high value. This high value allows data to be transmitted to the client more quickly and efficiently, especially in high latency networks. Providing better interactivity, faster file transfers, smoother video playback, higher framerate and resolution results in an enhanced user experience.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session interactivity is constantly measured to determine whether any data streams within the ICA session are adversely affecting interactivity. If that occurs, the throughput is decreased to reduce the impact of the large data stream on the session and allow interactivity to recover.

IMPORTANT:

HDX adaptive throughput changes the way that output buffers are set by moving this mechanism from the client to the VDA, and no manual configuration is necessary.

This feature has the following requirements:

- VDA version 1811 or later
- Workspace app for Windows 1811 or later

Improve the image quality sent to user devices

The following visual display policy settings control the quality of images sent from virtual desktops to user devices.

- Visual quality. Controls the visual quality of images displayed on the user device: medium, high, always lossless, build to lossless (default = medium). The actual video quality using the default setting of medium depends on available bandwidth.
- Target frame rate. Specifies the maximum number of frames per second that are sent from the virtual desktop to the user device (default = 30). For devices that have slower CPUs, specifying a lower value can improve the user experience. The maximum supported frame rate per second is 60.
- Display memory limit. Specifies the maximum video buffer size for the session in kilobytes (default = 65536 KB). For connections requiring more color depth and higher resolution, increase the limit. You can calculate the maximum memory required.

Improve video conference performance

Several popular video conferencing applications are optimized for delivery from Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) through multimedia redirection (see, for example, HDX RealTime Optimization Pack). For applications that are not optimized, HDX webcam video compression improves bandwidth efficiency and latency tolerance for webcams during video conferencing in a session. This technology streams webcam traffic over a dedicated multimedia

© 1997–2026 Citrix Systems, Inc. All rights reserved.

virtual channel. This technology uses less bandwidth compared to the isochronous HDX Plug-n-Play USB redirection support, and works well over WAN connections.

Citrix Workspace app users can override the default behavior by choosing the Desktop Viewer Mic & Webcam setting **Don't use my microphone or webcam**. To prevent users from switching from HDX webcam video compression, disable USB device redirection by using the policy settings under ICA policy settings > USB Devices policy settings.

HDX webcam video compression requires that the following policy settings be enabled (all are enabled by default).

- Client audio redirection
- Client microphone redirection
- Multimedia conferencing
- Windows Media Redirection

If a webcam supports hardware encoding, HDX video compression uses the hardware encoding by default. Hardware encoding might consume more bandwidth than software encoding. To force software compression, add the following DWORD key value to the registry key: `HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1`.

Network traffic priorities

Priorities are assigned to network traffic across multiple connections for a session using Quality of Service supported routers. Four TCP streams and two User Datagram Protocol (UDP) streams are available to carry ICA traffic between the user device and the server:

- TCP streams - real time, interactive, background, and bulk
- UDP streams - voice and Framehawk display remoting

Each virtual channel is associated with a specific priority and transported in the corresponding connection. You can set the channels independently, based on the TCP port number used for the connection.

Multiple channel streaming connections are supported for Virtual Delivery Agents (VDAs) installed on Windows 10 and Windows 8 machines. Work with your network administrator to ensure the Common Gateway Protocol (CGP) ports configured in the Multi-Port Policy setting are assigned correctly on the network routers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Quality of Service is supported only when multiple session reliability ports, or the CGP ports, are configured.

WARNING:

Use transport security when using this feature. Citrix recommends using Internet Protocol Security (IPsec) or Transport Layer Security (TLS). TLS connections are supported only when the connections traverse a NetScaler Gateway that supports multi-stream ICA. On an internal corporate network, multi-stream connections with TLS are not supported.

To set Quality of Service for multiple streaming connections, add the following Citrix policy settings to a policy (see Multi-stream connections policy settings for details):

- Multi-Port policy - This setting specifies ports for ICA traffic across multiple connections, and establishes network priorities.
  - Select a priority from the CGP default port priority list. By default, the primary port (2598) has a High priority.
  - Type more CGP ports in CGP port1, CGP port2, and CGP port3 as needed, and identify priorities for each. Each port must have a unique priority.

  Explicitly configure the firewalls on VDAs to allow the additional TCP traffic.
- Multi-Stream computer setting - This setting is disabled by default. If you use Citrix NetScaler SD-WAN with Multi-Stream support in your environment, you do not need to configure this setting. Configure this policy setting when using third-party routers or legacy Branch Repeaters to achieve the desired Quality of Service.
- Multi-Stream user setting - This setting is disabled by default.

For policies containing these settings to take effect, users must log off and then log on to the network.

Show or hide the remote language bar

The language bar displays the preferred input language in an application session. If this feature is enabled (default), you can show or hide the language bar from the **Advanced Preferences > Language bar** UI in Citrix Workspace app for Windows. By using a registry setting on the VDA side, you can disable client control of the language bar feature. If this feature is disabled, the client

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UI setting doesn't take effect, and the per user current setting determines the language bar state. For more information, see Improve the user experience.

To disable client control of the language bar feature from the VDA:

1. In the registry editor, navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`.
2. Create a DWORD value key, SeamlessFlags, and set it to 0x40000.

Unicode keyboard mapping

Non-Windows Citrix Receivers use the local keyboard layout (Unicode). If a user changes the local keyboard layout and the server keyboard layout (scan code), they might not be in sync and the output is incorrect. For example, User1 changes the local keyboard layout from English to German. User1 then changes the server-side keyboard to German. Even though both keyboard layouts are German, they might not be in sync causing incorrect character output.

Enable or disable Unicode keyboard layout mapping

By default, the feature is disabled on the VDA side. To enable the feature, toggle on the feature by using registry editor regedit on the VDA. Add the following registry key:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Name: EnableKlMap

Type: DWORD

Value: 1

To disable this feature, set **EnableKlMap** to 0 or delete the **CtxKlMap** key.

Enable Unicode keyboard layout mapping compatible mode

By default, Unicode keyboard layout mapping automatically hooks some windows API to reload the new Unicode keyboard layout map when you change the keyboard layout on the server side. A few applications cannot be hooked. To keep compatibility, you can change the feature to compatible mode to support these non-hooked applications. Add the following registry key:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Name: DisableWindowHook

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type: DWORD

Value: 1

To use normal Unicode keyboard layout mapping, set **DisableWindowHook** to 0.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix ICA® virtual channels

WARNING:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of a Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

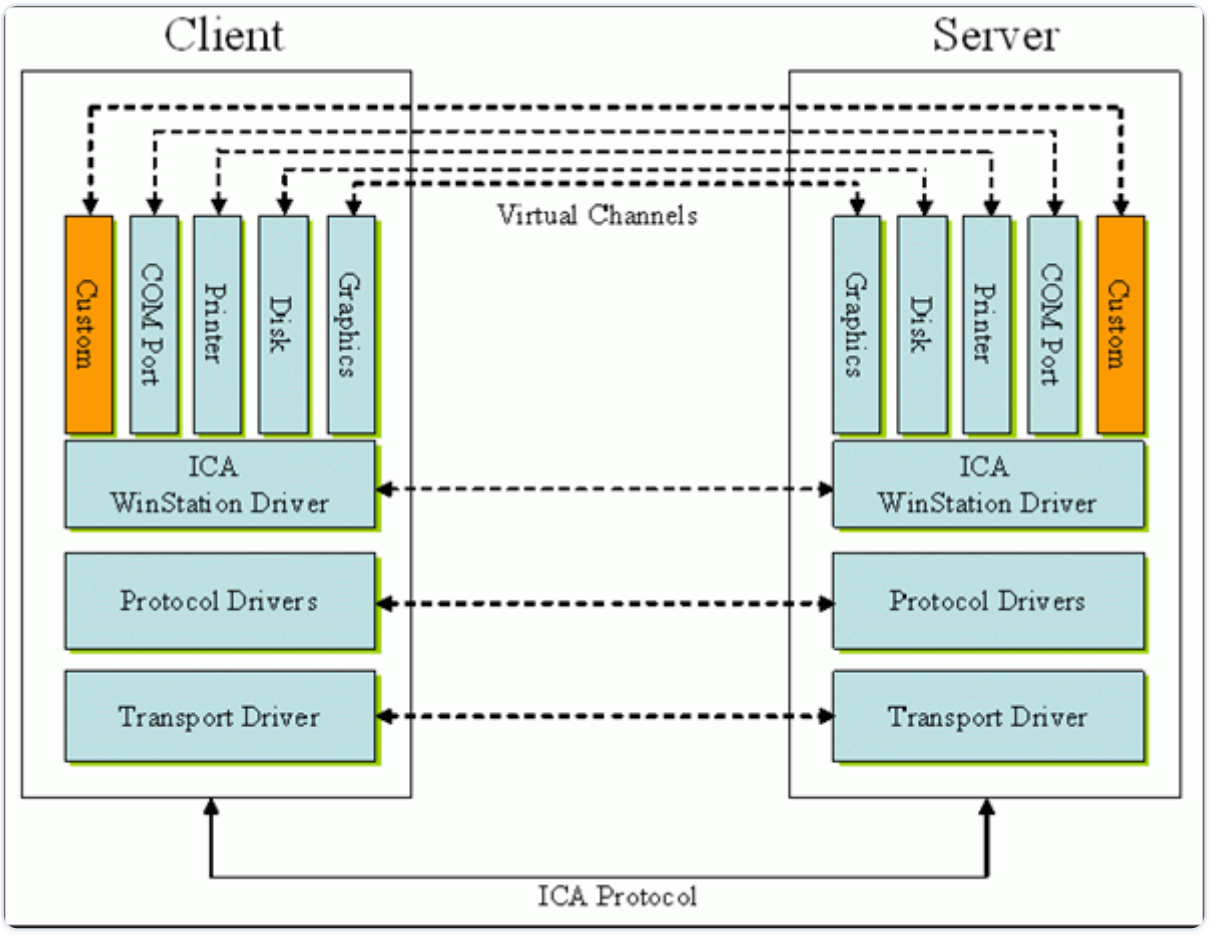
What are ICA virtual channels?

A large portion of the functionality and communication between the Citrix Workspace™ app and the Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) servers occurs over virtual channels. Virtual channels are a necessary part of the remote computing experience with the Citrix DaaS servers. Virtual channels are used for:

- Audio
- COM ports
- Disks
- Graphics
- LPT ports
- Printers
- Smart cards
- Third-party custom virtual channels
- Video

New virtual channels are sometimes released with Citrix DaaS™ and Citrix Workspace app products to provide more functionality.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A virtual channel consists of a client-side virtual driver that communicates with a server-side application. Citrix DaaS ships with various virtual channels included. They're designed to allow customers and third-party vendors to create their own virtual channels by using one of the provided Software Development Kits (SDKs).

Virtual channels provide a secure way to accomplish various tasks. For example, an application that is running on a Citrix Virtual Apps™ server that is communicating with a client-side device or an application that is communicating with the client-side environment.

On the client side, virtual channels correspond to virtual drivers. Each virtual driver provides a specific function. Some are required for normal operation, and others are optional. Virtual drivers operate at the presentation layer protocol level. There can be several protocols active at any time by multiplexing channels that are provided by the Windows Station (WinStation) protocol layer.

The following functions are contained in the VirtualDriver registry value under this registry path:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`

or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (for 64-bit)

- Thinwire3.0 (Required)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Clipboard
- ClientComm
- ClientAudio
- LicenseHandler (Required)
- TWI (Required)
- SmartCard
- ICACTL (Required)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

NOTE:

You can disable specific client functionality by removing one or more of these values from the registry key. For example, if you wanted to remove the Client Clipboard, remove the word **Clipboard**.

This list contains the client virtual driver files and their respective functions. Citrix Virtual Apps and Citrix Workspace app for Windows use these files. They are in the form of Dynamic Link Libraries (user mode), and not Windows drivers (kernel mode) except for Generic USB as described in Generic USB virtual channel.

- vd3dn.dll – Direct3D virtual channel used for desktop composition redirection
- vdcamN.dll – Bidirectional audio
- vdcdm30n.dll – Client drive mapping
- vdcom30N.dll - Client COM port mapping

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- vdcpm30N.dll – Client printer mapping
- vdctln.dll – ICA controls channel
- vddvc0n.dll – Dynamic virtual channel
- vdeuemn.dll - End user experience monitoring
- vdgusbn.dll – Generic USB virtual channel
- vdkbhook.dll – Transparent key pass-through
- vdlfpn.dll – Framehawk display channel over UDP like transport
- vdmmn.dll – Multimedia support
- vdmrvc.dll – Mobile Receiver virtual channel
- vdmtchn.dll - Multi-touch support
- vdscardn.dll – Smartcard support
- vdsens.dll – Sensors virtual channel
- vdspl30n.dll – Client UPD
- vdsspin.dll – Kerberos
- vdtuin.dll – Transparent UI
- vdtw30n.dll – Client Thinwire
- vdtwin.dll – Seamless
- vdtwn.dll – Twain

Some virtual channels are compiled into other files. For example Clipboard Mapping is available in wfica32.exe

64-bit compatibility

Citrix Workspace app for Windows is 64-bit compatible. As with most of the binaries compiled for 32 bit, these client files have 64-bit compiled equivalents:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

Generic USB virtual channel

Generic USB virtual channel implementation uses two kernel mode drivers along with virtual channel driver vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

How ICA virtual channels work

Virtual channels are loaded in multiple ways. The Shell (WfShell for the server and PicaShell for the workstation) load some virtual channels. Some virtual channels are hosted as windows services.

Virtual channel modules loaded by the Shell, for example:

- EUEM
- Twain
- Clipboard
- Multimedia
- Seamless session sharing
- Time Zone

Some are loaded as kernel mode, for example:

- CtxDvcs.sys – Dynamic virtual channel
- Icausbb.sys – Generic USB redirection
- Picadm.sys – Client drive mapping
- Picaser.sys – COM port redirection
- Picapar.sys – LPT port redirection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Graphics virtual channel on the server side

Starting with XenApp 7.0 and XenDesktop7.0, `ctxgfx.exe` hosts the graphics virtual channel for both workstation and terminal server based sessions. `Ctxgfx` hosts platform specific modules that interact with the corresponding driver (`Icardd.dll` for RDSH and `vdod.dll` and `vidd.dll` for workstation).

For XenDesktop® 3D Pro deployments an OEM graphics driver is installed for the corresponding GPU on the VDA. `Ctxgfx` loads specialized adaptor modules to interact with the OEM graphics driver.

Hosting specialized channels in windows services

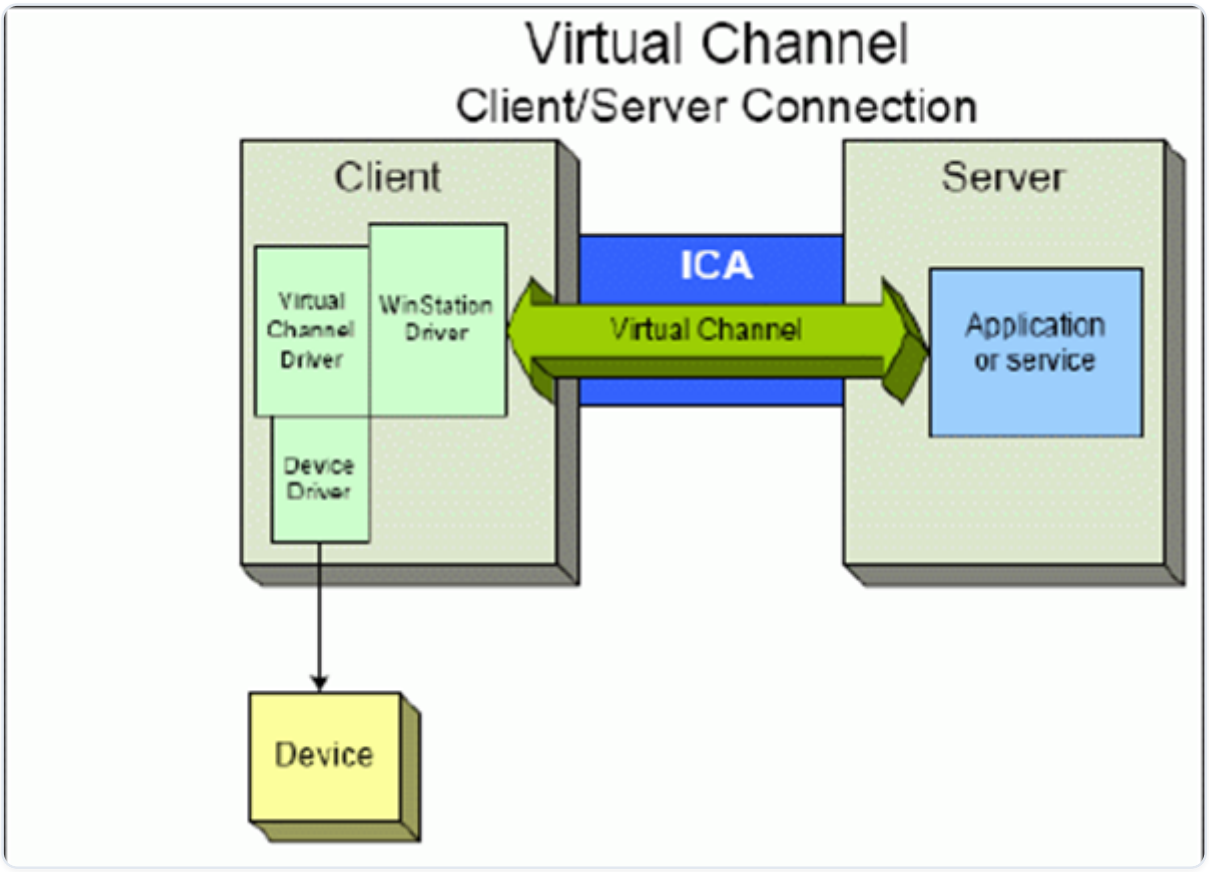
On Citrix DaaS servers, various channels are hosted as windows services. Such hosting provides one-to-many semantics for multiple applications in a session and multiple sessions on the server. Examples of such services include:

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service (Citrix Virtual Desktops™ only)
- Citrix ICA Status Channel Service

The audio virtual channel on Citrix Virtual Apps is hosted using Windows Audio service.

On the server side, all client virtual channels are routed through the WinStation driver, Wdica.sys. On the client side, the corresponding WinStation driver, built into wfica32.exe, polls the client virtual channels. This image illustrates the virtual channel client-server connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



This overview contains a client-server data exchange using a virtual channel.

1. The client connects to the Citrix DaaS server. The client passes information about the virtual channels it supports to the server.
2. The server-side application starts, obtains a handle to the virtual channel, and optionally queries for additional information about the channel.
3. The client virtual driver and server-side application pass data using the following two methods:
    - If the server application has data to send to the client, the data is sent to the client immediately. When the client receives the data, the WinStation driver de-multiplexes the virtual channel data from the ICA stream and immediately passes it to the client virtual driver.
    - If the client virtual driver has data to send to the server, the data is sent the next time the WinStation driver polls it. When the server receives the data, it is queued until the virtual channel application reads it. There is no way to alert the server virtual channel application that data was received.
4. When the server virtual channel application is completed, it closes the virtual channel and frees any allocated resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Creating your own virtual channel using the Virtual Channel SDK

Creating a virtual channel using the Virtual Channel SDK requires intermediate programming knowledge. Use this method to provide a major communication path between the client and the server. For example, if you are implementing usage of a device on the client side, such as a scanner, to be used with a process in the session.

NOTE:

- The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.
- Because of enhanced security for Citrix DaaS, you must specify which virtual channels are allowed to be opened in an ICA session. For more information, see Virtual channel allow list policy settings.

Creating your own virtual channel using the ICA Client Object SDK

Creating a virtual channel using the ICA Client Object (ICO) is easier than using the Virtual Channel SDK. Use the ICO by creating a named object in your program using the **CreateChannels** method.

IMPORTANT:

Because of enhanced security starting with the 10.00 version of the Citrix Receiver for Windows and later (and Citrix Workspace apps for Windows), you must take an extra step when creating an ICO virtual channel.

For more information, see Client Object API Specification Programmer's Guide.

Pass-through functionality of virtual channels

Most virtual channels that Citrix provides operate unmodified when you use the Citrix Workspace app for Windows within an ICA session (also known as a pass-through session). There are considerations when using the client in extra hops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following functions operate the same way in single or multiple hops:

- Client COM port mapping
- Client drive mapping
- Client printer mapping
- Client UPD
- End user experience monitoring
- Generic USB
- Kerberos
- Multimedia support
- Smartcard support
- Transparent key pass-through
- Twain

As the inherent nature of latency and factors such as compression and decompression and rendering being performed at each hop, performance might be affected with each additional hop that the client undergoes. The affected areas are:

- Bidirectional audio
- File transfers
- Generic USB redirection
- Seamless
- Thinwire

IMPORTANT:

By default, the client drives mapped by an instance of the client running in a pass-through session are restricted to the client drives of the connecting client.

Pass-through functionality of virtual channels between a Citrix Virtual Desktop session and a Citrix Virtual App session

Most virtual channels provided by Citrix operate unmodified when you use Citrix Workspace app for Windows within an ICA session on a Citrix Virtual Desktops server (also known as a pass-through session).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Specifically, on the Citrix Virtual Desktops server, there is a VDA hook that runs **picaPassthruHook**. This hook makes the client think it's running on a CPS server, and placing the client into its traditional pass-through mode.

We support the following traditional virtual channels and their functionality:

- Client
- Client COM port mapping
- Client drive mapping
- Client printer mapping
- Generic USB (limited due to performance)
- Multimedia support
- Smartcard support
- SSON
- Transparent key pass-through

Security and ICA virtual channels

Securing usage is an important part of planning, developing, and implementing virtual channels. There are several references to specific areas of security located throughout this document.

Best practices

Open virtual channels when you **Connect** and **Reconnect**. Close virtual channels when you log off and **Disconnect**.

Keep the following guidelines in mind when you create scripts that use virtual channel functions.

Naming the Virtual Channels:

You can create a maximum of 32 virtual channels. Seventeen of the 32 channels are reserved for special purposes.

- Virtual channel names must not be more than seven characters in length.
- The first three characters are reserved for the vendor name, and the next four for the channel type. For example, **CTXAUD** represents the Citrix audio virtual channel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual channels are referred to by a seven-character (or shorter) ASCII name. In some previous versions of the ICA protocol, virtual channels were numbered. The numbers are now assigned dynamically based on the ASCII name, making implementation easier. Users who are developing virtual channel code for internal use only can use any seven-character name that does not conflict with existing virtual channels. Use only numbers and upper and lowercase ASCII. Follow the existing naming convention when adding your own virtual channels. There are several predefined channels. The predefined channels begin with the OEM identifier CTX and are for use only by Citrix.

Double-Hop Support:

VIRTUAL CHANNEL	IS DOUBLE HOP SUPPORTED?
Audio	No
Browser Content Redirection	No
CDM	Yes
CEIP	No
Clipboard	Yes
Continuum (MRVC)	No
Control VC	Yes
HTML5 Video Redirection (v1)	Yes
Keyboard, Mouse	Yes
MultiTouch	No
NSAPVC	No
Printing	Yes
SensVC	No
Smartcard	Yes
Twain	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIRTUAL CHANNEL	IS DOUBLE HOP SUPPORTED?
USB VC	Yes
WAYCOM devices -K2M using USB VC	Yes
Webcam Video Compression	Yes
Windows Media Redirection	Yes

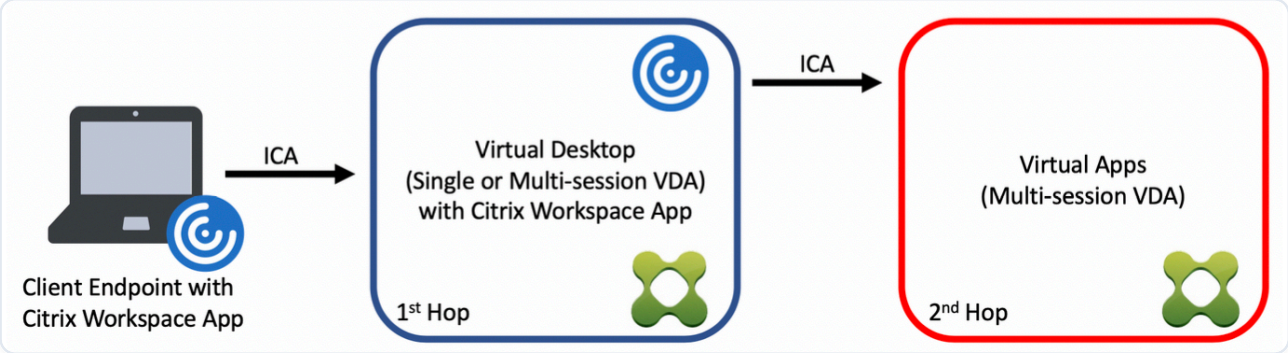
See also

- ICA Virtual Channel SDK
- The Citrix Developer Network is the home for all technical resources and discussions involving the use of Citrix SDKs. In this network, you can find access to SDKs, sample code and scripts, extensions and plug-ins, and SDK documentation. Also included are the Citrix Developer Network forums, where technical discussions take place around each of the Citrix SDKs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Double hop in Citrix DaaS™

In the context of a Citrix client session, the term “double hop” refers to a Citrix Virtual App session that is running within a Citrix Virtual Desktop session. The following diagram illustrates a double hop.



In a double hop scenario, when the user connects to a Citrix Virtual Desktop running on a single-session OS VDA (known as VDI) or a multi-session OS VDA (known as a published desktop), that is considered the first hop. After the user connects to the virtual desktop, the user can launch a Citrix Virtual Apps™ session. That is considered the second hop.

You can use a double hop deployment model to support various use cases. The case where the Citrix Virtual Desktop and the Citrix Virtual Apps environments are managed by different entities is one common example. This method can also be effective in resolving application compatibility issues.

System requirements

All Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) editions support double hop.

The first hop must use a supported version of the single-session or multi-session OS VDA and the Citrix Workspace App. The second hop must use a supported version of the multi-session OS VDA. See the Product Matrix page for supported versions.

For best performance and compatibility, Citrix recommends using a Citrix client of the same version or newer than the VDA versions in use.

In environments where the first hop involves a third-party (non-Citrix) virtual desktop solution in combination with a Citrix Virtual Apps session, support is limited to the Citrix Virtual Apps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

environment. In the event of any issues related to the third-party virtual desktop, including - but not limited to - Citrix Workspace™ app compatibility, redirection of hardware devices, and session performance, Citrix can provide technical support in a limited capacity. A Citrix Virtual Desktop at the first hop might be required as part of troubleshooting.

Deployment considerations for HDX™ in double hop

In general, each session in a double hop is unique and client-server functions are isolated to a given hop. This section includes areas that require special consideration by Citrix administrators. Citrix recommends that customers conduct thorough testing of required HDX capabilities to ensure user experience and performance is adequate for a given environment configuration.

Graphics

Use default graphics settings (selective encoding) on the first and second hops. In the case of HDX 3D Pro, Citrix highly recommends that all applications that require graphics acceleration run locally in the first hop with the appropriate GPU resources available to the VDA.

Latency

End-to-end latency can impact the overall user experience. Consider the added latency between the first and second hops. This is especially important with redirection of hardware devices.

Multimedia

Server-side (in session) rendering of audio and video content performs best in the first hop. Video playback in the second hop requires decoding and re-encoding at the first hop, increasing bandwidth and hardware resource utilization as a result. Audio and video content must be limited to the first hop whenever possible.

USB device redirection

HDX includes generic and optimized redirection modes to support a wide array of USB device types. Pay special attention to the mode in use at each hop and use the following table as reference for best results. For more information about generic and optimized redirection modes, see Generic USB devices.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIRST HOP (VDI OR PUBLISHED DESKTOP)	SECOND HOP (VIRTUAL APPS)	SUPPORT NOTES
Optimized	Optimized	Recommended (based on device support). For example, USB mass storage, TWAIN scanners, Webcam, Audio.
Generic	Generic	For devices where the optimized option is not available.
Generic	Optimized	While technically possible, it is recommended to use the optimized mode across both hops when device support is available.
Optimized	Generic	Not supported

NOTE:

Due to the inherent chattiness of USB protocols, performance may decrease across hops. Functionality and results vary depending on specific device and application requirements. Validation testing is highly recommended in all cases of device redirection and especially important in double hop scenarios.

Support exceptions

Double hop sessions support most HDX features and capabilities except for the following:

- Browser content redirection
- Local App Access
- RealTime Optimization Pack for Skype for Business
- Optimization for Microsoft Teams

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX™ connectivity

Citrix HDX represents a broad set of technologies that deliver a high-definition experience to users of centralized applications and desktops, on any device and over any network.

HDX is designed around three technical principles:

- Intelligent redirection
- Adaptive compression
- Data de-duplication

Applied in different combinations, they optimize the IT and user experience, decrease bandwidth consumption, and increase user density per hosting server.

Within the HDX offering, you can connect over a unique, proprietary transport protocol, utilize the maximum transmission units when establishing sessions, and optimize connectivity with Citrix SD-WAN.

Adaptive transport

Adaptive Transport is a mechanism in Citrix Virtual Apps and Desktops™ that allows establishing connections for HDX sessions using a preferred transport protocol while providing a fallback to TCP if connectivity with the preferred protocol is unavailable.

The following transport protocols are supported:

- Enlightened Data Transport (EDT)
- Transmission Control Protocol (TCP)

Configuration

Adaptive Transport is enabled by default. You can configure Adaptive Transport to operate in the following modes:

- **Preferred**: (Default) The client attempts to connect with the preferred protocol and falls back to TCP if connectivity with the preferred protocol is unavailable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

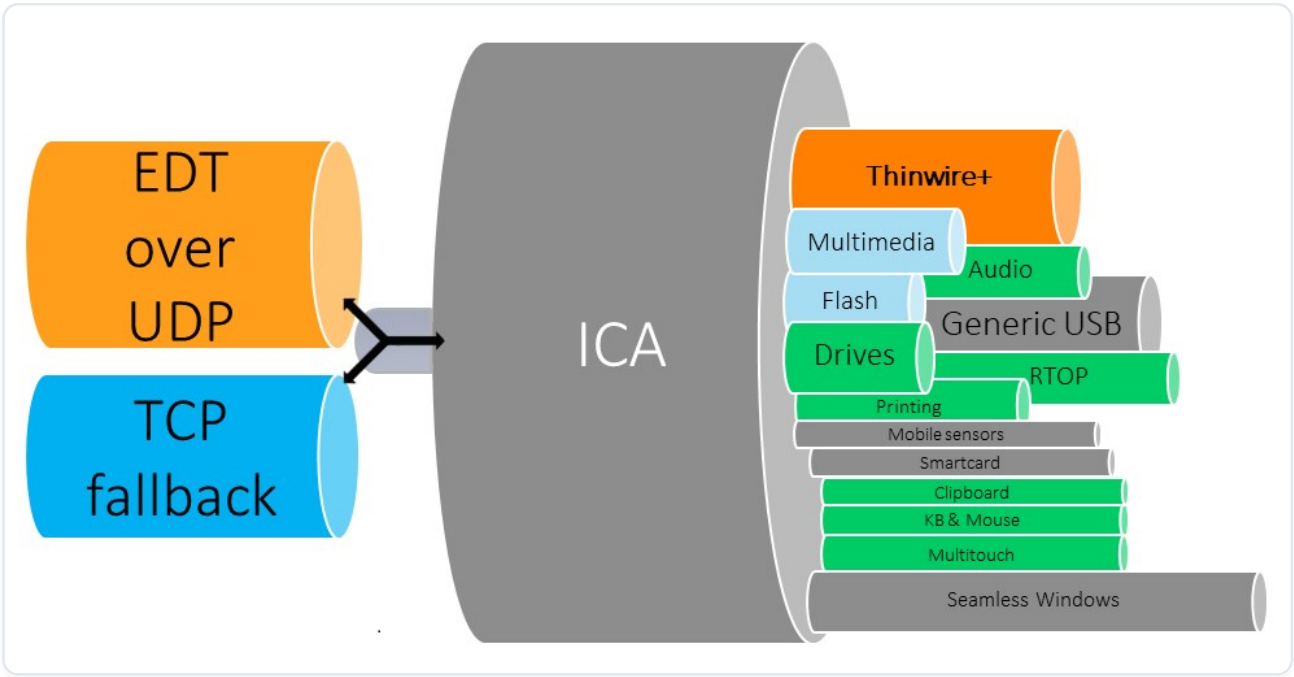
- **Diagnostic mode**: The client only attempts to connect using the preferred protocol. Fall back to TCP is disabled.
- **Off**: The client only attempts to connect using TCP.

How it works

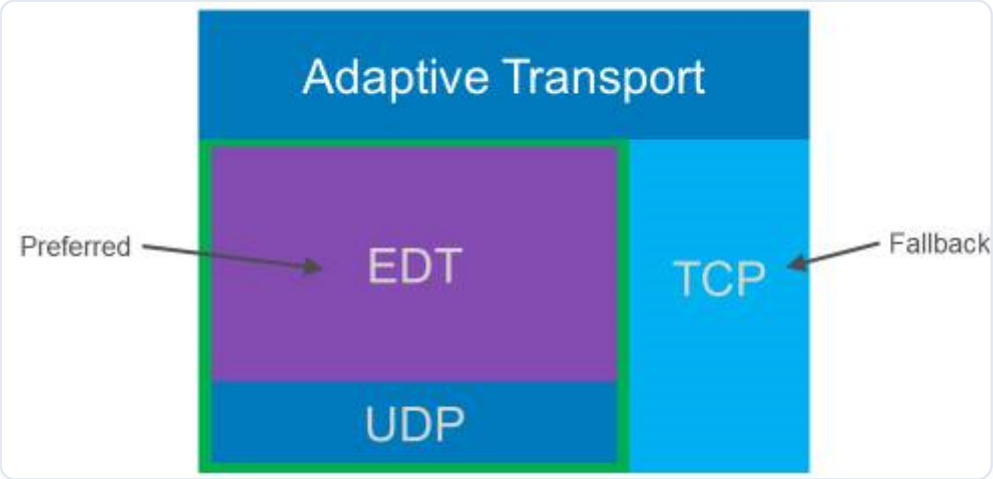
When **Adaptive Transport** is set to `Preferred`, the client attempts to connect to the session with both the preferred protocol and TCP in parallel. This allows optimizing the connection time if it's not possible to connect with the preferred protocol and the client must fall back to using TCP. If the connection is established using TCP, the client attempts to connect with the preferred protocol in the background every five minutes.

When **Adaptive Transport** is set to `Diagnostic mode`, the client connects to the session only with the preferred protocol. If the client is unable to establish a connection using the preferred protocol, it doesn't fall back to using TCP, and the connection fails.

When **Adaptive Transport** is set to `Off`, **Adaptive Transport** is disabled, and the client connects to the session using TCP only.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



System requirements

The following are the requirements for using Adaptive Transport and EDT:

- Control plane
  - Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
  - Citrix Virtual Apps and Desktops: currently supported version
- Virtual Delivery Agent
  - Windows: currently supported version (2402 or later recommended)
  - Linux: currently supported version (2402 or later recommended)
- Citrix Workspace™ app
  - Windows: currently supported version (2402 or later recommended)
  - Linux: currently supported version (2402 or later recommended)
  - Mac: currently supported version (2402 or later recommended)
  - iOS: latest version available in the Apple App Store
  - Android: latest version available in Google Play
- Citrix NetScaler® Gateway
  - 14.1.12.30 or later (recommended)
  - 13.1.17.42 or later (13.1-52.19 or later recommended)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For details on Linux VDA, please see the Linux Virtual Delivery Agent documentation.

Network requirements

The following sections are the network requirements for using EDT with Adaptive Transport:

Session hosts

If your session hosts have a firewall such as Windows Defender Firewall, you must allow the following inbound traffic for internal connections.

DESCRIPTION	SOURCE	PROTOCOL	PORT
Internal connection - Session Reliability enabled	Client	UDP	2598
Internal connection - Session Reliability disabled			1494
Internal connection - HDX™ Direct or VDA SSL			443

NOTE:

The VDA installer adds the appropriate inbound rules to the Windows Defender Firewall. If you use a different firewall, you must add the rules above.

Internal network

The following table depicts the firewall rules required for using EDT in your network:

DESCRIPTION	PROTOCOL	SOURCE	DESTINATION	DESTINATION PORT
Direct internal connection - Session	UDP	Client network	VDA network	2598

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DESCRIPTION	PROTOCOL	SOURCE	DESTINATION	DESTINATION PORT
Reliability enabled				
Direct internal connection - Session Reliability disabled				1494
Direct internal connection - HDX Direct or VDA SSL				443
NetScaler Gateway		NetScaler SNIP		2598
NetScaler Gateway - VDA SSL				443

NOTE:

If you are using Citrix Gateway Service, you must enable **Rendezvous** to use EDT as your transport protocol. See the Rendezvous documentation for system and network requirements.

Client network

The following table outlines the connectivity requirements for client devices:

DESCRIPTION	PROTOCOL	SOURCE	DESTINATION	DESTINATION PORT
Internal connection - Session Reliability enabled	UDP	Client IP	VDA network	2598

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DESCRIPTION	PROTOCOL	SOURCE	DESTINATION	DESTINATION PORT
Internal connection - Session Reliability disabled				1494
Internal connection - HDX Direct or SSL VDA				443
External connection - NetScaler Gateway			NetScaler Gateway public IP address	443
External connection - Citrix Gateway Service			Citrix Gateway Service	443

NOTE:

If you are using Citrix Gateway Service, clients must be able to reach `<https://*.*.nssvc.net>`. If you can't allow all subdomains using `<https://*.*.nssvc.net>`, you can use `<https://*.c.nssvc.net>` and `<https://*.g.nssvc.net>` instead. For more information, see Knowledge Center article CTX270584.

Enlightened Data Transport

Enlightened Data Transport (EDT) is a Citrix-proprietary transport protocol built on top of User Datagram Protocol (UDP). It delivers a superior user experience on challenging long-haul connections while maintaining server scalability. EDT improves data throughput for all ICA® virtual channels on unreliable networks, providing a better and more consistent user experience.

When **Adaptive Transport** is enabled, EDT is the preferred protocol.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Things to know

- **Session Reliability** must be enabled to use **MTU Discovery** and EDT with NetScaler® Gateway and Citrix Gateway Service.
- Packet fragmentation can cause performance degradation or even failure to open sessions in some cases. To prevent this, you must adjust the EDT MTU to a value adequate for your networks. You can use EDT MTU Discovery or a manual workaround described in How to configure MSS when using EDT on networks with non-standard MTU.
- For details on enabling the use of EDT with NetScaler Gateway, see Configure NetScaler Gateway to support Enlightened Data Transport.

EDT MTU Discovery

MTU Discovery allows EDT to automatically determine the Maximum Transmission Unit (MTU) when establishing a session. Doing so prevents EDT packet fragmentation that might result in performance degradation or failure to establish a session.

MTU Discovery is enabled by default. If you need to disable it, see HDX features managed through the registry for details.

NOTE:

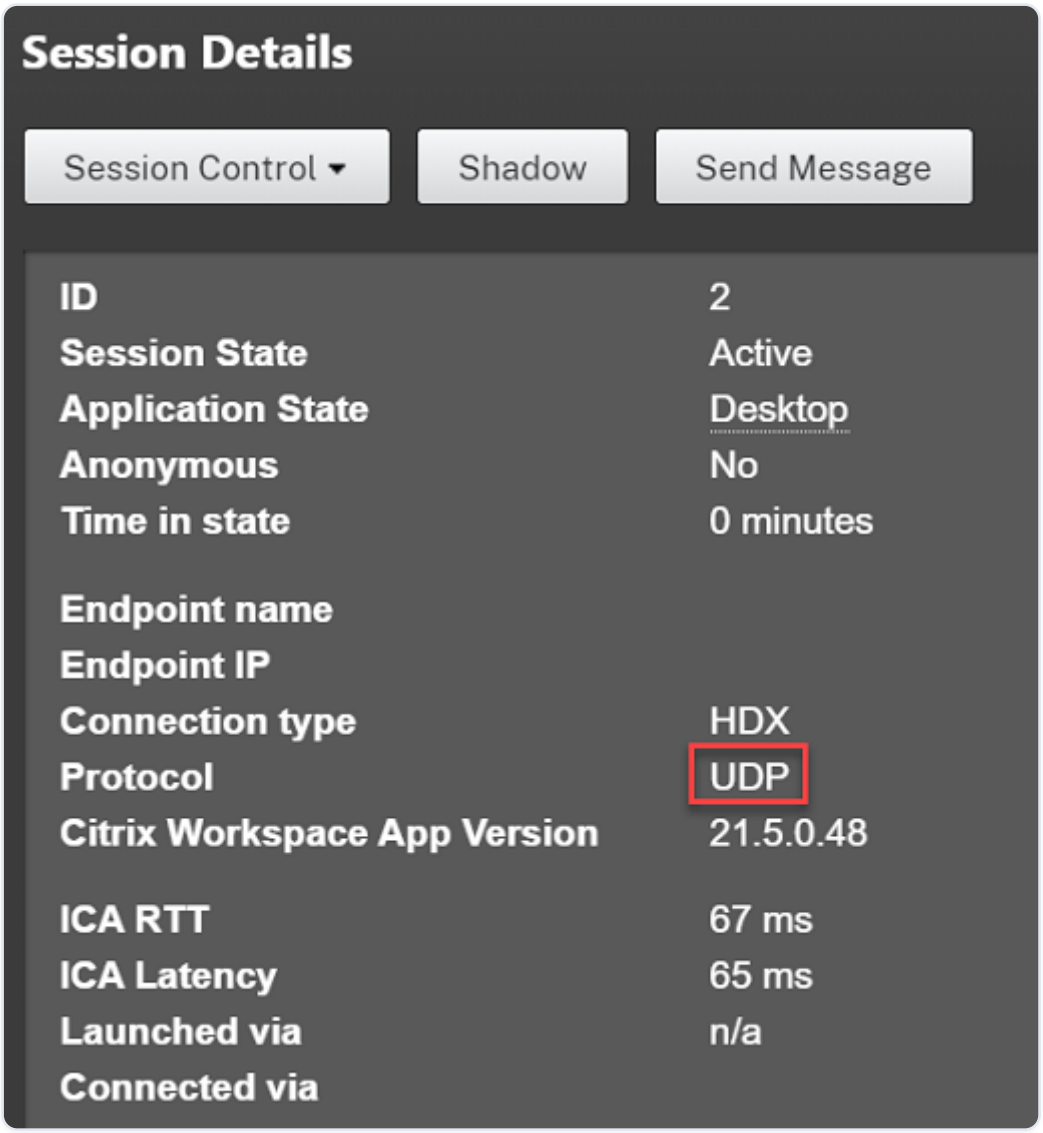
- **Session Reliability** must be enabled for MTU Discovery to work.
- MTU Discovery with Multi-Stream ICA is available with VDA versions 2209 and later.

Troubleshooting

To confirm that EDT is being used as the transport protocol for the session, you can use Director or the `CtxSession.exe` command-line utility on the VDA.

In Director, look up the session and select **Details**. If the **Connection type** is `HDX` and the **Protocol** is `UDP`, EDT is being used as the transport protocol for the session.

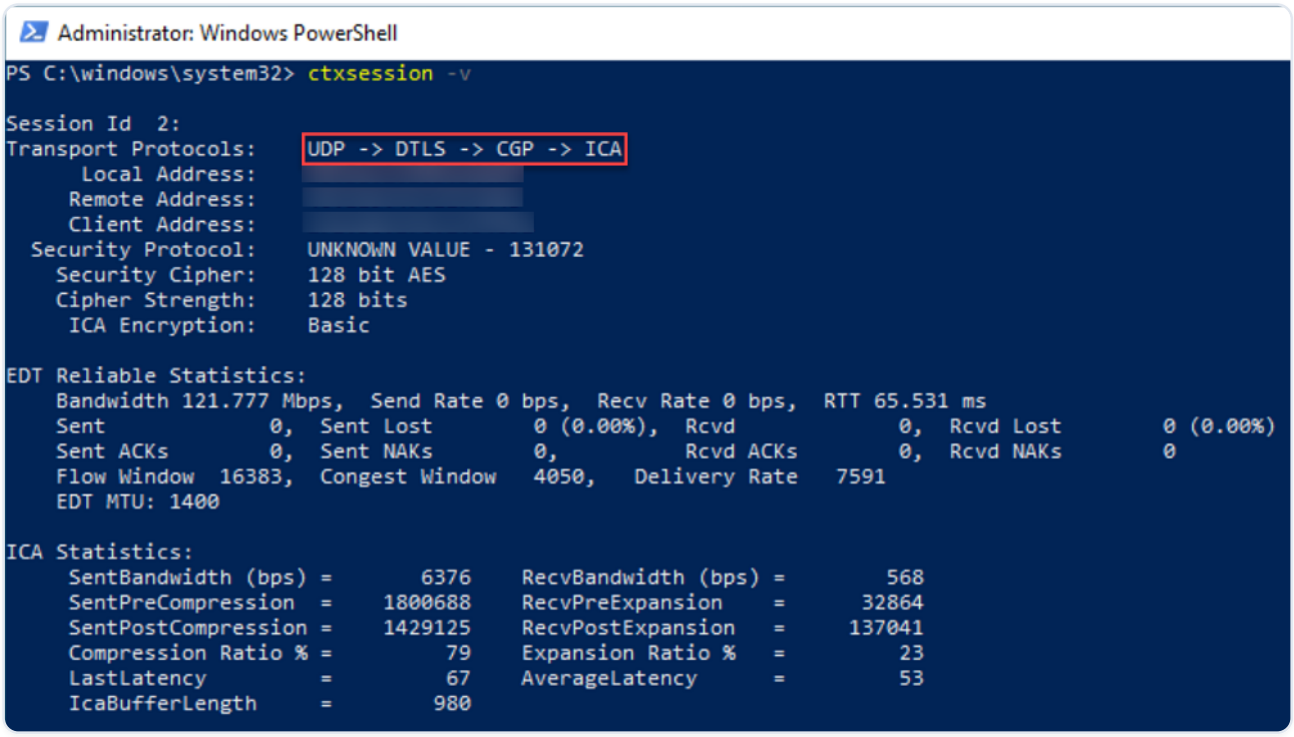
© 1997–2026 Citrix Systems, Inc. All rights reserved.



To use the CtxSession.exe utility, launch a Command Prompt or PowerShell within the session and run `ctxsession.exe`. To see verbose statistics, run `ctxsession.exe -v`. If EDT is in use, the transport protocol shows one of the following:

- **UDP > ICA®** (Session Reliability disabled)
- **UDP > CGP > ICA** (Session Reliability enabled)
- **UDP > DTLS > CGP > ICA** (ICA is DTLS-encrypted end-to-end)

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When sessions fail to connect with EDT

To troubleshoot **Adaptive Transport** and **EDT**, we suggest the following:

1. Review the System requirements, Network requirements, Known issues, and Things to know, and ensure that all items have been addressed.
2. Check if there are Citrix® policies in Studio or GPO overwriting the desired **HDX Adaptive Transport** setting.
3. Check if there are settings on the client overwriting the desired HDX Adaptive Transport setting. This can be a GPO preference, a setting configured using the optional Workspace app administrative template, or a manual configuration of the **HDXoverUDP** setting in the registry or client's configuration file.
4. On multi-session VDA machines, ensure that the UDP listeners are active. Open a command prompt in the VDA machine and run `netstat -a -p udp`. For more information, see How to Confirm HDX Enlightened Data Transport Protocol.
5. Check if the appropriate firewall rules have been configured in both network firewalls and firewalls running on the VDA machines.
6. Launch a direct session internally, bypassing the NetScaler® Gateway or Citrix Gateway Service, and check the protocol in use. If the session uses EDT, the VDA is ready to use EDT for external connections through NetScaler Gateway or Citrix Gateway Service.
7. If EDT works for direct internal connections and not for sessions going through NetScaler Gateway or Citrix Gateway Service:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ensure that **Session Reliability** is enabled.
- If using NetScaler Gateway, ensure that your configuration adheres to the required configuration outlined in Configure NetScaler Gateway to support Enlightened Data Transport and HDX Insight.

8. If using Citrix Gateway Service, ensure that Rendezvous is enabled and working.
9. Check if your users' connections require a non-standard MTU. Connections with an effective MTU lower than 1500 bytes cause EDT packet fragmentation, which in turn can affect performance or even cause session launch failures. This issue is common when using VPNs, some Wi-Fi access points, and mobile networks, such as 4G and 5G. Ensure that you either have MTU Discovery enabled or are setting a custom MTU as outlined in How to configure MSS when using EDT on networks with non-standing MTU.

Known issues

- Asymmetrical network paths can cause MTU Discovery to fail for connections that do not go through NetScaler Gateway or Citrix Gateway Service. To address this issue, upgrade to VDA version 2103 or later.
- When using NetScaler Gateway, asymmetrical network paths can cause MTU Discovery to fail. This is due to an issue on Gateway that causes the Don't Fragment (DF) bit in the EDT packets' header not to be propagated. A fix for this issue is available, starting with firmware release 13.1 build 17.42. For details on how to enable the fix, see the NetScaler Gateway documentation.
- MTU Discovery can fail for users that connect through a DS-Lite network. Some modems fail to honor the DF bit when packet processing is enabled, preventing MTU Discovery from detecting fragmentation. In this situation, the following are the available options:
  - Disable packet processing on the user's modem.
  - Disable **MTU Discovery** and use a hardcoded MTU as described in How to configure MSS when using EDT on networks with non-standing MTU.
  - Disable **Adaptive Transport** to force sessions to use TCP. If only a subset of users are affected, consider disabling it on the client side so that other users can continue to use EDT.

Rendezvous protocol

When using the Citrix Gateway Service, the Rendezvous protocol allows VDAs to bypass the Citrix Cloud™ Connectors to connect directly and securely with the Citrix Cloud control plane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

There are two types of traffic to consider:

1. Control traffic for VDA registration and session brokering.
2. HDX™ session traffic.

There are two versions of Rendezvous available:

- Version 1 (V1): supports bypassing the Citrix Cloud Connectors for HDX session traffic only.
- Version 2 (V2): supports bypassing the Citrix Cloud Connectors for both control traffic and HDX session traffic.

For details about system requirements, considerations, and configuration for each of the Rendezvous versions, review their respective documentation.

Rendezvous V1 documentation

Rendezvous V2 documentation

Rendezvous V1

When using the Citrix Gateway Service, the Rendezvous protocol allows VDAs to bypass the Citrix Cloud™ Connectors to connect directly and securely with the Citrix Cloud control plane.

Requirements

- Access to environment using Citrix® StoreFront Cloud and Citrix Gateway service.
- Control Plane: Citrix DaaS™ (Citrix Cloud).
- VDA: Version 1912 or later.
  - Version 2012 is the minimum required for EDT Rendezvous.
  - Version 2012 is the minimum required for non-transparent proxy support (no PAC file support).
  - Version 2103 is the minimum required for proxy configuration with a PAC file.
- Enable the Rendezvous protocol in the Citrix policy. For more information, see Rendezvous protocol policy setting.
- The VDAs must have access to `https://*.nssvc.net`, including all subdomains. If you can't add all subdomains to the allow list in that manner, use `https://*.c.nssvc.net` and `https://*.g.nssvc.net` instead. For more information, see the Internet Connectivity Requirements section of the Citrix Cloud documentation (under Citrix DaaS) and the Knowledge Center article CTX270584.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The VDAs must be able to connect to the addresses mentioned previously on TCP 443 and UDP 443 for TCP Rendezvous and EDT Rendezvous, respectively.
- Cloud Connectors must obtain the VDAs' FQDNs when brokering a session. Accomplish this task in one of these two ways:
  - **Enable DNS resolution for the site.** Navigate to **Settings > Site settings** and turn on the **Enable DNS resolution** setting. Alternatively, use the Citrix Virtual Apps and Desktops Remote PowerShell SDK and run the command `Set-BrokerSite -DnsResolutionEnabled $true`. For more information about the Citrix Virtual Apps and Desktops Remote PowerShell SDK, see SDKs and APIs.
  - **DNS Reverse Lookup Zone with PTR records for the VDAs.** If you choose this option, we recommend that you configure VDAs to always attempt to register PTR records. To do so, use the Group Policy Editor or Group Policy Object, navigate to **Computer Configuration > Administrative Templates > Network > DNS Client**, and set **Register PTR Records** to **Enabled and Register**. If the connection's DNS suffix does not match the domain's DNS suffix, you must also configure the **Connection-specific DNS suffix** setting for the machines to register PTR records successfully.

NOTE:

If using the DNS resolution option, the Cloud Connectors must be able to resolve the fully qualified domain names (FQDNs) of the VDA machines. In the case that internal users connect directly to the VDA machines, the client devices also must be able to resolve the VDA machines' FQDNs.

If using a DNS reverse lookup zone, the FQDNs in the PTR records must match the FQDNs of the VDA machines. If the PTR record contains a different FQDN, the Rendezvous connection fails. For example, if the machine's FQDN is `vda01.domain.net`, the PTR record must contain `vda01.domain.net`. A different FQDN such as `vda01.sub.domain.net` does not work.

Proxy configuration

The VDA supports establishing Rendezvous connections through a proxy.

Proxy considerations

Consider the following when using proxies with Rendezvous:

- Transparent proxies, non-transparent HTTP proxies, and SOCKS5 proxies are supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Packet decryption and inspection are not supported. Configure an exception so that the ICA® traffic between the VDA and the Gateway Service is not intercepted, decrypted, or inspected. Otherwise, the connection breaks.
- HTTP proxies support machine-based authentication by using Negotiate and Kerberos or NT LAN Manager (NTLM) authentication protocols.

  When you connect to the proxy server, the Negotiate authentication scheme automatically selects the Kerberos protocol. If Kerberos isn't supported, Negotiate falls back to NTLM for authentication.

  NOTE:

  To use Kerberos, you must create the service principal name (SPN) for the proxy server and associate it with the proxy's Active Directory account. The VDA generates the SPN in the format `HTTP/<proxyURL>` when establishing a session, where the proxy URL is retrieved from the **Rendezvous proxy** policy setting. If you don't create an SPN, authentication falls back to NTLM. In both cases, the VDA machine's identity is used for authentication.

- Authentication with a SOCKS5 proxy is not currently supported. If using a SOCKS5 proxy, you must configure an exception so that traffic destined to Gateway Service addresses (specified in the requirements) can bypass authentication.
- Only SOCKS5 proxies support data transport through EDT. For an HTTP proxy, use TCP as the transport protocol for ICA.

Transparent proxy

If using a transparent proxy in your network, no additional configuration is required on the VDA.

Non-transparent proxy

If using a non-transparent proxy in your network, configure the Rendezvous proxy configuration setting. When the setting is enabled, specify the HTTP or SOCKS5 proxy address, or enter the path to the PAC file so the VDA knows which proxy to use. For example:

- Proxy address: `http://<URL or IP>:<port>` or `socks5://<URL or IP>:<port>`
- PAC file: `http://<URL or IP>/<path>/<filename>.pac`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you use the PAC file to configure the proxy, define the proxy using the syntax required by the Windows HTTP service: `PROXY [<scheme>=]<URL or IP>:<port>`. For example, `PROXY socks5=<URL or IP>:<port>`.

Rendezvous validation

If you meet all requirements, follow these steps to validate if Rendezvous is in use:

1. Launch PowerShell or a command prompt within the HDX™ session.
2. Run `ctxsession.exe –v`.
3. The transport protocols in use indicate the type of connection:
    - TCP Rendezvous: **TCP > SSL > CGP > ICA**
    - EDT Rendezvous: **UDP > DTLS > CGP > ICA**
    - Proxy through Cloud Connector: **TCP > CGP > ICA**

Other considerations

Windows cipher suite order

For a custom cipher suite order, make sure that you include the VDA-supported cipher suites from the following list:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

If the custom cipher suite order does not contain these cipher suites, the Rendezvous connection fails.

Zscaler Private Access

If using Zscaler Private Access (ZPA), it is recommended that you configure bypass settings for the Gateway Service to avoid increased latency and the associated performance impact. To do so, you must define application segments for the Gateway Service addresses – specified in the requirements – and set them to always bypass. For information on configuring application segments to bypass ZPA, see the Zscaler documentation.

Rendezvous V2

When using the Citrix Gateway Service, the Rendezvous protocol allows VDAs to bypass the Citrix Cloud™ Connectors to connect directly and securely with the Citrix Cloud control plane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Rendezvous V2 is supported with standard domain joined machines, Microsoft Entra hybrid joined machines, Microsoft Entra joined machines, and non-domain joined machines.

NOTE:

Currently, connectorless deployments are possible with *Azure AD joined* and *non-domain joined* machines only. Standard AD domain joined machines and Microsoft Entra hybrid joined machines still require Cloud Connectors for VDA registration and session brokering. However, there are no DNS requirements for using Rendezvous V2.

Cloud Connector requirements for other functions not related to VDA communication, such as connecting to your on-prem AD domain, MCS provisioniong to on-prem hypervisors, etc., remain the same.

Requirements

The requirements for using Rendezvous V2 are:

- Access to the environment using Citrix® StoreFront Cloud and Citrix Gateway Service
- Control plane: Citrix DaaS™
- VDA version 2203
- Enable the Rendezvous protocol in the Citrix policy. For more information, see Rendezvous protocol policy setting.
- Session Reliability must be enabled on the VDAs
- The VDA machines must have access to:
  - `https://*.xendesktop.net` on `TCP 443`. If you can't allow all subdomains in that manner, you can use `https://<customer_ID>.xendesktop.net`, where \<customer_ID\> is your Citrix Cloud customer ID as shown in the Citrix Cloud administrator portal.
  - `https://*.*.nssvc.net` on `TCP 443` for the control connection with Gateway Service.
  - `https://*.*.nssvc.net` on `TCP 443` and `UDP 443` for HDX sessions over TCP and EDT, respectively.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you can't allow all subdomains using `https://*.*.nssvc.net`, you can use `https://*.c.nssvc.net` and `https://*.g.nssvc.net` instead. For more information, see Knowledge Center article CTX270584.

Proxy configuration

The VDA supports connecting through proxies for both control traffic and HDX™ session traffic when using Rendezvous. The requirements and considerations for both types of traffic are different, so review them carefully.

Control traffic proxy considerations

- Only HTTP proxies are supported.
- Packet decryption and inspection are not supported. Configure an exception so the control traffic between the VDA and the Citrix Cloud control plane is not intercepted, decrypted, or inspected. Otherwise, the connection fails.
- Machine-based authentication is supported only if the VDA machine is AD domain joined. It can use Negotiate/Kerberos or NTLM authentication.

NOTE:

To use Kerberos, create the service principal name (SPN) for the proxy server and associate it with the proxy's Active Directory account. The VDA generates the SPN in the format `HTTP/<proxyURL>` when establishing a connection with Citrix Cloud. If you don't create an SPN, authentication falls back to NTLM. In both cases, the VDA machine's identity is used for authentication.

HDX traffic proxy considerations

- HTTP and SOCKS5 proxies are supported.
- EDT can only be used with SOCKS5 proxies.
- By default, HDX traffic uses the proxy defined for control traffic. If you must use a different proxy for HDX traffic, whether a different HTTP proxy or a SOCKS5 proxy, use the Rendezvous proxy configuration policy setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Packet decryption and inspection are not supported. Configure an exception so the HDX traffic between the VDA and the Citrix Cloud control plane is not intercepted, decrypted, or inspected. Otherwise, the connection fails.
- Machine-based authentication is supported only with HTTP proxies and if the VDA machine is AD domain joined. It can use Negotiate/Kerberos or NTLM authentication.

  NOTE:

  To use Kerberos, create the service principal name (SPN) for the proxy server and associate it with the proxy's Active Directory account. The VDA generates the SPN in the format `HTTP/<proxyURL>` when establishing a session, where the proxy URL is retrieved from the Rendezvous proxy configuration policy setting. If you don't create an SPN, authentication falls back to NTLM. In both cases, the VDA machine's identity is used for authentication.

- Authentication with a SOCKS5 proxy is not currently supported. If using a SOCKS5 proxy, configure an exception so that traffic destined to Gateway Service addresses (specified in the requirements) can bypass authentication.
- Only SOCKS5 proxies support data transport through EDT. For an HTTP proxy, use TCP as the transport protocol for ICA.

Transparent proxy

If using a transparent proxy in your network, no additional configuration is required on the VDA.

Non-transparent proxy

If using a non-transparent proxy in your network, specify the proxy during the VDA installation so that control traffic can reach the Citrix Cloud control plane. Make sure to review the control traffic proxy considerations before proceeding with the installation and configuration.

In the VDA installation wizard, select **Rendezvous Proxy Configuration** in the **Additional Components** page. This option makes the **Rendezvous Proxy Configuration** page available later in the installation wizard. Once here, enter the proxy address or the path to the PAC file for the VDA to know which proxy to use. For example:

- Proxy address: `http://<URL or IP>:<port>`
- PAC file: `http://<URL or IP>/<path/<filename>.pac`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

As stated in the HDX traffic proxy considerations, HDX traffic uses the proxy defined during the VDA installation by default. If you must use a different proxy for HDX traffic, whether a different HTTP proxy or a SOCKS5 proxy, use the Rendezvous proxy configuration policy setting. When the setting is enabled, specify the HTTP or SOCKS5 proxy address. You can also enter the path to the PAC file so the VDA knows which proxy to use. For example:

- Proxy address: `http://<URL or IP>:<port>` or `socks5://<URL or IP>:<port>`
- PAC file: `http://<URL or IP>/<path/<filename>.pac`

If you use the PAC file to configure the proxy, define the proxy using the syntax required by the Windows HTTP service: `PROXY [<scheme>=]<URL or IP>:<port>`. For example, `PROXY socks5=<URL or IP>:<port>.`

How to configure Rendezvous

Following are the steps for configuring Rendezvous in your environment:

1. Make sure that all requirements are met.
2. If you must use a non-transparent HTTP proxy in your environment, configure it during the VDA installation. Refer to the proxy configuration section for details.
3. Reboot the VDA machine after installation is complete.
4. Create a Citrix policy, or edit an existing one:
    - Set the **Rendezvous Protocol** setting to **Allowed**.
    - If you must configure an HTTP or SOCKS5 proxy for HDX traffic, configure the **Rendezvous proxy configuration** setting.
    - Ensure that the Citrix policy filters are set properly. The policy applies to the machines that need Rendezvous enabled.
5. Ensure that the Citrix policy has the correct priority so that it does not overwrite another one.

NOTE:

If you are using VDA version 2308 or older, V1 is used by default. For more information on how to configure the version to use, see HDX features managed through the registry.

Rendezvous validation

If you meet all requirements and have completed the configuration, follow these steps to validate if Rendezvous is in use:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Within the virtual desktop, open a command prompt or PowerShell.
2. Run `ctxsession.exe -v`.
3. The transport protocols displayed indicate the type of connection:
    - TCP Rendezvous: TCP > SSL > CGP > ICA
    - EDT Rendezvous: UDP > DTLS > CGP > ICA
    - Not Rendezvous: TCP > CGP > ICA
4. The Rendezvous version reported indicates the version in use.

Other considerations

Windows cipher suite order

If the cipher suite order has been modified in the VDA machines, make sure that you include the VDA-supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

If the custom cipher suite order does not contain these cipher suites, the Rendezvous connection fails.

Zscaler Private Access

If using Zscaler Private Access (ZPA), it is recommended that you configure bypass settings for the Gateway Service to avoid increased latency and the associated performance impact. To do so, you must define application segments for the Gateway Service addresses – specified in the requirements – and set them to always bypass. For information on configuring application segments to bypass ZPA, see the Zscaler documentation.

Known Issues

VDA 2203 installer does not allow entering a slash (/) for the proxy address

As a workaround, you can configure the proxy in the registry after the VDA is installed:

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent

Value type: String
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Value name: ProxySettings

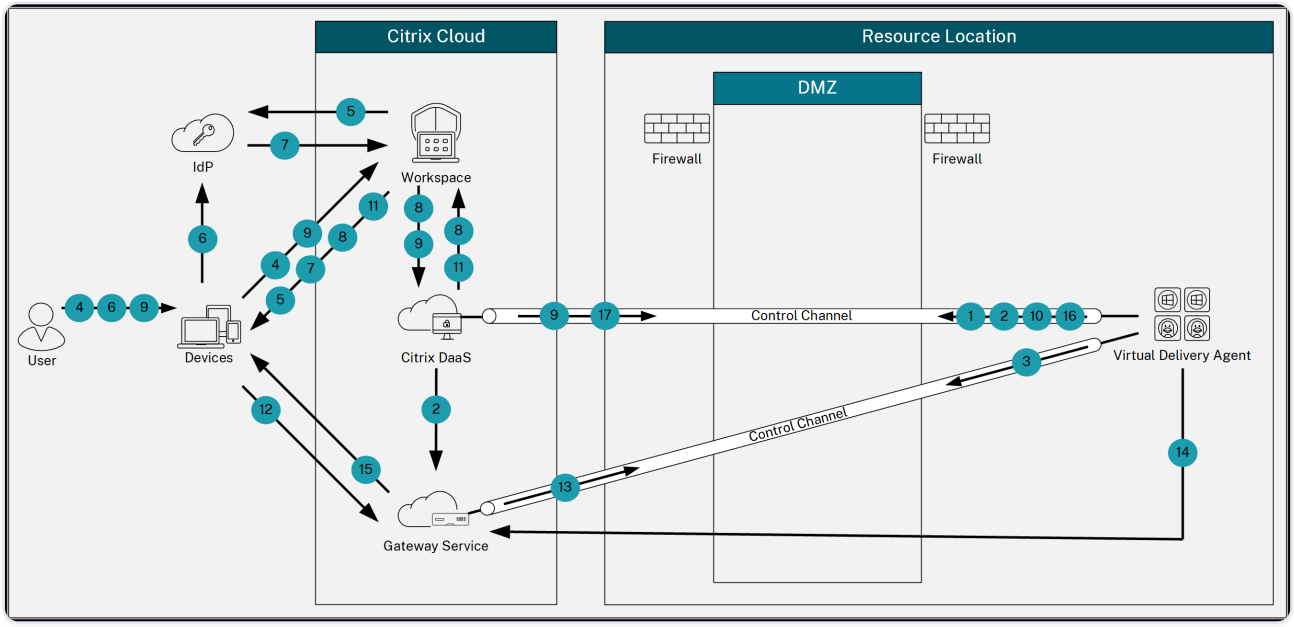
Value data: Proxy address or path to pac file. For example:

    Proxy address: http://squidk.test.local:3128

    Pac file: http://file.test.com/config/proxy.pac
```

Rendezvous traffic flow

The following diagram illustrates the sequence of steps about Rendezvous traffic flow.



1. The VDA establishes a WebSocket connection with Citrix Cloud and registers.
2. The VDA registers with Citrix Gateway Service and obtains a dedicated token.
3. The VDA establishes a persistent control connection with the Gateway Service.
4. The user navigates to their store URL.
5. Citrix® StoreFront Cloud evaluates authentication configuration and redirects users to the appropriate IdP for authentication.
6. The user enters their credentials.
7. After successfully validating the user credentials, the user is redirected to Citrix® StoreFront Cloud.
8. Citrix® StoreFront Cloud counts resources for the user and displays them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. The user selects a desktop or application from the store. Citrix® StoreFront Cloud sends the request to Citrix DaaS, which brokers the connection and instructs the VDA to prepare for the session.
10. The VDA responds with the Rendezvous capability and its identity.
11. Citrix DaaS generates a launch ticket and sends it to the user device through Citrix® StoreFront Cloud.
12. The user's endpoint connects to the Gateway Service and provides the launch ticket to authenticate and identify the resource to connect to.
13. The Gateway Service sends the connection information to the VDA.
14. The VDA establishes a direct connection for the session with the Gateway Service.
15. The Gateway Service completes the connection between the endpoint and the VDA.
16. The VDA verifies licensing for the session.
17. Citrix DaaS sends applicable policies to the VDA.

HDX™ Direct

When accessing Citrix-delivered resources, HDX Direct allows both internal and external client devices to establish a secure direct connection with the session host if direct communication is possible.

System requirements

The following are the system requirements for using HDX Direct:

- Control plane
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2503 or later
- Virtual Delivery Agent (VDA)
  - Windows: version 2503 or later
- Workspace app
  - Windows: version 2503 or later
  - Linux: version 2411 or later
  - Mac: version 2411 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Access tier
  - Citrix® StoreFront Cloud
  - Citrix StoreFront 2503 or later
  - Citrix Gateway Service
  - Citrix NetScaler® Gateway

Network requirements

The following are the network requirements for using HDX Direct.

Session hosts

If your session hosts have a firewall such as Windows Defender Firewall, you must allow the following inbound traffic for internal connections.

DESCRIPTION	SOURCE	PROTOCOL	PORT
Direct internal connection	Client	TCP	443
Direct internal connection	Client	UDP	443

Note:

> The VDA installer adds the appropriate inbound rules to Windows Defender Firewall. If you use a different firewall, you must add the rules above.

Client network

The following table describes the client network for internal and external users.

Internal users

DESCRIPTION	PROTOCOL	SOURCE	SOURCE PORT	DESTINATION	DESTINATION PORT
Direct internal connection	TCP	Client network	1024–65535	VDA network	443

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DESCRIPTION	PROTOCOL	SOURCE	SOURCE PORT	DESTINATION	DESTINATION PORT
Direct internal connection	UDP	Client network	1024–65535	VDA network	443

External users

DESCRIPTION	PROTOCOL	SOURCE	SOURCE PORT	DESTINATION	DESTINATION PORT
STUN (external users only)	UDP	Client network	1024–65535	Internet (see note below)	3478, 19302
External user connection	UDP	Client network	1024–65535	Data center's public IP address	1024–65535

Data center network

The following table describes the data center network for internal and external users.

Internal users

DESCRIPTION	PROTOCOL	SOURCE	SOURCE PORT	DESTINATION	DESTINATION PORT
Direct internal connection	TCP	Client network	1024–65535	VDA network	443
Direct internal connection	UDP	Client network	1024–65535	VDA network	443

© 1997–2026 Citrix Systems, Inc. All rights reserved.

External users

DESCRIPTION	PROTOCOL	SOURCE	SOURCE PORT	DESTINATION	DESTINATION PORT
STUN (external users only)	UDP	VDA network	1024–65535	Internet (see note below)	3478, 19302
External user connection	UDP	DMZ / Internal network	1024–65535	VDA network	55000–55250
External user connection	UDP	VDA network	55000–55250	Client's public IP	1024–65535

NOTE:

Both the VDA and Workspace app attempt to send STUN requests to the following servers in the same order:

- stun.cloud.com:3478
- stun.cloudflare.com:3478
- stun.l.google.com:19302

If you change the default port range for external user connections using the **HDX Direct port range** policy setting, the corresponding firewall rules must match your custom port range.

Configuration

HDX Direct is disabled by default. You can configure this feature using the **HDX Direct** setting in the Citrix policy.

- **HDX Direct**: To enable or disable a feature.
- **HDX Direct mode**: Determines if **HDX Direct** is available for internal clients only or for both internal and external clients.
- **HDX Direct port range**: Defines the port range that the VDA uses for connections from external clients.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If needed, the list of STUN servers used by HDX Direct can be modified by editing the following registry value:

- Key: HKLM\SOFTWARE\Citrix\HDX-Direct
- Value type: REG_MULTI_SZ
- Value name: STUNServers
- Data: stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

NOTE:

HDX Direct for external users is only available with EDT (UDP) as the transport protocol. Therefore, Adaptive Transport must be enabled.

Considerations

The following are considerations for using HDX Direct:

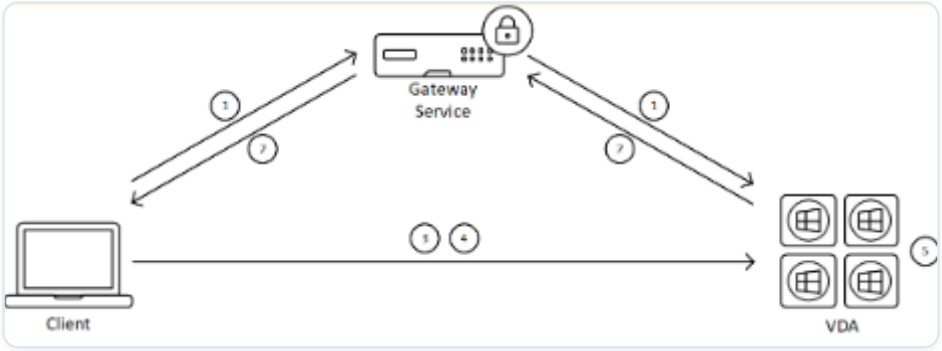
- HDX Direct for external users is only available with EDT (UDP) as the transport protocol. Therefore, **Adaptive Transport** must be enabled.
- If you are using **HDX Insight**, note that using **HDX Direct** prevents the HDX Insight data collection, as the session would no longer be proxied through NetScaler Gateway.

How it works

HDX Direct allows clients to establish a direct connection to the session host when direct communication is available. When direct connections are made using HDX Direct, self-signed certificates are used to secure the direct connection with network level-encryption (TLS/DTLS).

Internal users

The following diagram depicts the overview of the HDX Direct connection process of internal users.



1. The client establishes an HDX session through the Gateway Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Upon a successful connection, the VDA sends to the client the VDA machine's FQDN, a list of its IP addresses, and the VDA machine's certificate via the HDX connection.
3. The client probes the IP addresses to see if it can reach the VDA directly.
4. If the client can reach the VDA directly with any of the IP addresses shared, the client establishes a direct connection with the VDA, secured with (D)TLS using a certificate that matches the one exchanged in step (2).
5. Once the direct connection is successfully established, the session is transferred to the new connection, and the connection to the Gateway Service is terminated.

NOTE:

After establishing the connection in step 2, above, the session is active. The subsequent steps do not delay or interfere with the user's ability to use the virtual application or desktop. If any of the subsequent steps fail, the connection through the Gateway is maintained without interrupting the user's session.

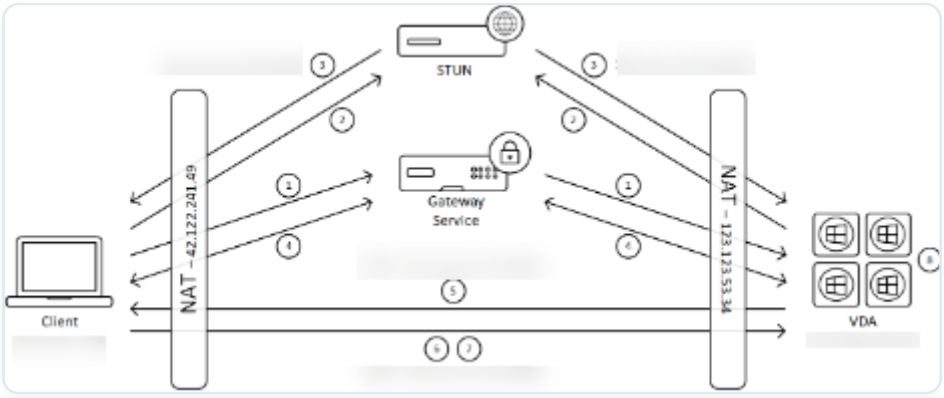
Traditional direct connections

When using Storefront, Workspace with Direct Workload Connection, or Workspace configured for internal-only connectivity, direct connections are established between the client and the session host without the need to route through a Gateway first.

In these instances, HDX Direct is not triggered since the connections are inherently direct. However, if HDX Direct is enabled, these connections will leverage the HDX Direct certificates to secure the sessions.

External users

The following diagram depicts the overview of the HDX Direct connection process for external users:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. The client establishes an HDX session through the Gateway Service.
2. Upon a successful connection, both the client and the VDA send a STUN request to discover their public IP addresses and ports.
3. The STUN server responds to the client and VDA with their corresponding public IP addresses and ports.
4. Through the HDX connection, the client and the VDA exchange their public IP addresses and UDP ports, and the VDA sends its certificate to the client.
5. The VDA sends UDP packets to the client's public IP address and UDP port. The client sends UDP packets to the VDA's public IP address and UDP port.
6. Upon receipt of a message from the VDA, the client responds with a secure connection request.
7. During the DTLS handshake, the client verifies that the certificate matches the certificate exchanged in step (4). After validation, the client sends its authorization token. A secure direct connection is now established.
8. Once the direct connection is successfully established, the session is transferred to the new connection, and the connection to the Gateway Service is terminated.

NOTE:

After establishing the connection in step 2, above, the session is active. The subsequent steps do not delay or interfere with the user's ability to use the virtual application or desktop. If any of the subsequent steps fail, the connection through the Gateway is maintained without interrupting the user's session.

Certificate management

Overview

HDX™ Direct connections are secured with network level encryption. To facilitate this, each session host has a unique self-signed root CA certificate and a corresponding server certificate, which is signed by the self-signed root CA certificate.

This solution provides the following advantages:

- **Streamlined Security:** HDX Direct connections are secured without the administrative overhead of managing certificates within the environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Reduced Attack Surface:** The attack surface is limited to a single host because each host has a unique set of keys and certificates.
- **Enhanced Security for Non-Persistent Environments:** In environments with non-persistent session hosts, security is further enhanced as new keys and certificates are generated upon restart.

Session host

The **Citrix ClxMtp Service** and the **Citrix Certificate Manager Service** are the two services responsible for managing certificates on each session host. The ClxMtp Service handles key generation and rotation, while the Certificate Manager Service generates and manages the certificates.

Two certificates are created: a self-signed root CA and a server certificate. Both are issued with a two-year validity period; however, they are replaced when keys are rotated. Additionally, new certificates are generated each time non-persistent machines restart.

Details for each certificate are as follows:

- **Self-signed Root CA**
  - Issued to: CA-Citrix-Certificate-Manager
  - Issued by: CA-Citrix-Certificate-Manager
  - Issuer details: The organization is Citrix Systems, Inc.
- **Server Certificate**
  - Issued to: \<host FQDN\> (For example, FTLW11-001.ctxlab.net)
  - Issued by: CA-Citrix-Certificate-Manager
  - Issuer details: The organization is Citrix Systems, Inc.

NOTE:

The Citrix Certificate Manager Service generates RSA certificates that leverage 2048-bit keys.

If there is an existing machine certificate created by the Citrix Certificate Manager Service and the subject name does not match the machine's FQDN, a new certificate is generated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Key rotation

The **Citrix ClxMtp Service** automatically rotates keys every six months. However, you can trigger a key rotation manually by increasing the rotation counter in the session host's registry.

To rotate the keys, update the following value:

- Key: SOFTWARE\Citrix\ClxMtpConnectorSvcRotateKeyPairs
- Value type: DWORD
- Value name: ClxMtpRotateRequestCounter
- Data: integer (Decimal)

NOTE:

For first-time key rotation:

1. Create the ClxMtpConnectorSvcRotateKeyPairs key.
2. Create and set the ClxMtpRotateRequestCounter value to 1.

For subsequent key rotations, increase the ClxMtpRotateRequestCounter value by 1.
Once the value is updated, the **Citrix ClxMtp Service** will automatically rotate the keys without requiring a restart. The **Citrix Certificate Manager Service** will then generate new certificates automatically once it detects new keys.

Client device

The root CA certificate is sent to the client by Citrix® StoreFront Cloud or Citrix® StoreFront through the already established secure and trusted connection path. This eliminates the need to distribute CA certificates to the client devices' certificate stores, and ensures that the client trusts the certificates used to secure the HDX Direct connection.

Using custom certificates

HDX Direct supports the use of certificates issued and managed by your own PKI. The following steps outline how to install your certificate, configure the necessary permissions, bind it to the session manager service, and enable the required TLS listeners.

1. Proceed to step 2 if HDX Direct is disabled on the machine. If HDX Direct is enabled, follow the steps below:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

   a. Open the registry editor (regedit.exe) and navigate to **HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**.
   b. Set the **SSLEnabled** value to **0**.
   c. Navigate to **HKLM\Software\Citrix\HDX-Direct**.
   d. Set the **HdxDirectCaInTls** value to **0**.

2. Install the appropriate certificate issued by your PKI on the machine's certificate store.
3. Grant the session manager service read access to the certificate's private keys.
   a. Launch the Microsoft management console (**MMC**): Start > Run > mmc.exe.
   b. Navigate to **File > Add/Remove Snap-in**.
   c. Select **Certificates**, then click **Add**.
   d. Choose **Computer account** and click **Next**.
   e. Select **Local computer** and click **Finish**.
   f. Navigate to **Certificates (Local Computer) > Personal > Certificates**.
   g. Right click on the appropriate certificate and select **All Tasks > Manage Private Keys**.
   h. Add one of the following services and give it Read access:
      - For **Single Session VDA**: `NT SERVICE\PorticaService`
      - For **Multi Session VDA**: `NT SERVICE\TermService`
   i. Click **Apply**, then **OK**.
4. Bind the certificate to the session manager service.
   a. Retrieve the certificate thumbprint (double click on the certificate > **Details** > **Thumbprint**).
   b. Open the registry editor (regedit.exe) and navigate to **HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**.
   c. Edit the **SSLThumbprint** value and paste the certificate's thumbprint.
5. Enable the Citrix TLS listeners.
   a. In the same registry location, set the **SSLEnabled** value to **1**.
6. Enable HDX Direct (in Citrix policy).

The Citrix Virtual Apps and Desktops installation media includes a PowerShell script (Enable-VdaSSL.ps1) that automates several of these tasks:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Setting permissions for the certificate's keys
- Binding the certificate to the session manager service
- Enabling the Citrix TLS listeners

This script is located in the Support > Tools > SslSupport directory. For more details, see Configure TLS on a VDA using the PowerShell script.

NOTE:

The devices connecting to the session hosts need to have the correct root CA and intermediate CA certificates installed if you are using your own certificates.

NAT Compatibility

To establish a direct connection between an external user device and the session host, HDX™ Direct leverages hole punching for NAT traversal and STUN to facilitate the exchange of the public IP address and port mappings for the client device and session host. This is similar to how VoIP, unified communications, and P2P solutions work.

As long as firewalls and other network components are configured to allow the UDP traffic for the STUN requests and the HDX sessions, HDX Direct for external users is expected to work. However, there are certain scenarios where the NAT types of the user and session host networks lead to an incompatible combination, thus causing HDX Direct to fail.

Validations

You can validate the NAT type and filtering on the client and the session host by using STUNTMAN's STUN client utility:

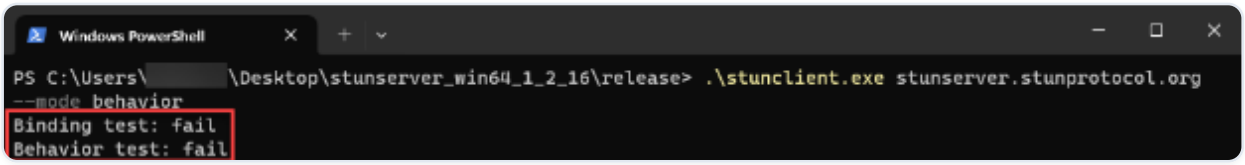
1. Download the appropriate package for the target platform from stunprotocol.org, and extract the contents.
2. Open a terminal prompt and navigate to the directory where the contents were extracted.
3. Run the following command: `.\stunclient.exe stunserver.stunprotocol.org --mode behavior`
4. Take note of the output.

   If the binding and behavior tests are successful, both **binding test** and **behavior test** report the success and a NAT behavior is specified:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If the tests fail, both **binding test** and **behavior test** report the failure.



5. Run the following command: `.\stunclient.exe stunserver2024.stunprotocol.org --mode filtering`
6. Take note of the output.

See the following table to determine if HDX Direct for external users is expected to work based on the test results of both the client and session host:

CLIENT NAT BEHAVIOR	CLIENT NAT FILTERING	SESSION HOST NAT BEHAVIOR	SESSION HOST NAT FILTERING	EXPECTED TO WORK?
Endpoint Independent Mapping	Any	Endpoint Independent Mapping	Any	Yes
Endpoint Independent Mapping	Endpoint Independent Filtering	Address Dedependent Mapping	Any	Yes
Endpoint Independent Mapping	Address Dependent Filtering	Address Dedependent Mapping	Any	No
Endpoint Independent Mapping	Address and Port Dependent Filtering	Address Dedependent Mapping	Any	No
Endpoint Independent Mapping	Endpoint Independent Filtering	Address and Port Dedependent Mapping	Endpoint Independent Filtering	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CLIENT NAT BEHAVIOR	CLIENT NAT FILTERING	SESSION HOST NAT BEHAVIOR	SESSION HOST NAT FILTERING	EXPECTED TO WORK?
Endpoint Independent Mapping	Address Dependent Filtering	Address Dedependent Mapping	Any	No
Endpoint Independent Mapping	Address and Port Dependent Filtering	Address Dedependent Mapping	Any	No
Address Dependent Mapping	Any	Endpoint Independent Mapping	Endpoint Independent Filtering	Yes
Address Dependent Mapping	Any	Endpoint Independent Mapping	Address Dependent Filtering	No
Address Dependent Mapping	Any	Endpoint Independent Mapping	Address and Port Dependent Filtering	No
Address Dependent Mapping	Any	Address Dependent Mapping	Any	No
Address Dependent Mapping	Any	Address and Port Dependent Mapping	Any	No
Address and Port Dependent Mapping	Any	Endpoint Independent Mapping	Endpoint Independent Filtering	Yes
Address and Port Dependent Mapping	Any	Endpoint Independent Mapping	Address Dependent Filtering	No
Address and Port Dependent Mapping	Any	Endpoint Independent Mapping	Address and Port Dependent Filtering	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

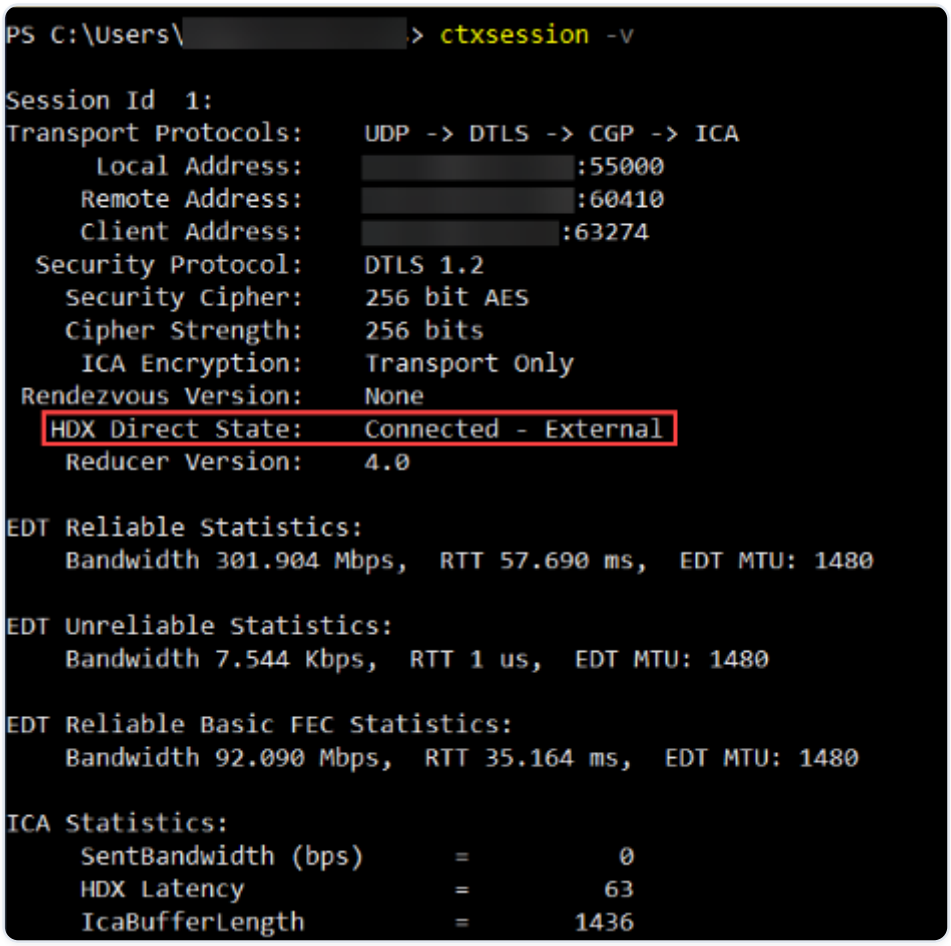
CLIENT NAT BEHAVIOR	CLIENT NAT FILTERING	SESSION HOST NAT BEHAVIOR	SESSION HOST NAT FILTERING	EXPECTED TO WORK?
Address and Port Dependent Mapping	Any	Address Dependent Mapping	Any	No
Address and Port Dependent Mapping	Any	Address and Port Dependent Mapping	Any	No
Fail	Any	Any	Any	No
Any	Any	Fail	Any	No
Fail	Any	Fail	Any	No

Troubleshooting

To confirm that **HDX Direct** successfully established a direct connection, you can use the `CtxSession.exe` utility on the VDA machine.

To use the `CtxSession.exe` utility, launch a Command Prompt or PowerShell within the session and run `ctxsession.exe -v`. If the **HDX Direct** connection is successfully established, **HDX Direct Status** is `Connected`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can also look at the session host's event logs for information on whether the HDX™ Direct connection was established successfully or failed. See the **Event Logs** section for details.

Note:

> Depending on the environment and the number of IP addresses available to the session hosts, it can take up to 5 minutes for the HDX Direct connection to be established.

When HDX Direct fails to establish a direct connection

If HDX Direct is failing to establish a direct connection, review the following steps:

1. Ensure that the VDA version and Workspace app version in use support the feature per the system requirements.
2. Confirm that you have a policy applied to the VDA that enables HDX Direct and that there are no other policies with higher priority disabling the feature.
3. Confirm that you have a policy applied to the VDA that sets the desired HDX Direct mode and that there are no other policies with higher priority overwriting the configuration.
4. Ensure that the Citrix ClxMtp Service is running on the session host.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Ensure that the Citrix Certificate Manager Service is running on the session host. If it's not running, try to start it manually. The service automatically stops if HDX Direct is disabled.
6. Check if the session host has its self-signed Root CA certificate:
    a. Issued to: `CA-<hostname>` (For example, CA-FTLW11-001)
    b. Issued by: `CA-<hostname>` (For example, CA-FTLW11-001)
    c. Issuer details: The organization is Citrix Systems, Inc.
7. Check if the session host has its self-signed server certificate:
    a. Issued to: `<host FQDN>` (For example, FTLW11-001.ctxlab.net)
    b. Issued by: `CA-<hostname>` (For example, CA-FTLW11-001)
    c. Issuer details: The organization is Citrix Systems, Inc.
8. If the certificates are missing, contact Citrix Tech Support.
9. If the certificates are present:
    a. Stop the Citrix Certificate Manager Service on the session host.
    b. Delete both the self-signed Root CA certificate and the self-signed server certificate.
    c. Start the Citrix Certificate Manager Service on the session host. The service creates new certificates once it starts.
10. For internal users:
    a. Ensure the session host's firewall is not blocking inbound traffic on UDP 443 or TCP 443, for HDX over EDT and HDX over TCP, respectively.
    b. Ensure that your network firewall is not blocking traffic on UDP 443 and TCP 443 between your clients' network and session hosts' network.
11. For external users:
    a. Check the NAT type for the client and the session host, and ensure that the combination is expected to work. See the NAT Compatibility section for details.
    b. If the NAT test fails on either the client or the session host:
        i. If there is a firewall running on the system, ensure it is not blocking outbound traffic on UDP 3478.
        ii. Ensure that your network firewalls are not blocking outbound traffic on UDP 3478.
        iii. Ensure the firewalls are not blocking the STUN server's response.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Ensure that your network firewalls have the appropriate rules configured to allow all necessary traffic. See the Network Requirements section for details.

d. If you change the default port range using the HDX Direct port range policy setting, ensure that your firewall rules are set for the custom port range.

Event logs

The following events are logged in the VDA machine's event log:

LOG	ID	SOURCE	LEVEL	DESCRIPTION
Applications and Services Logs > Citrix-HostCore-HDX Direct/ Operational	1	HDX Direct	Information	HDX Direct connection for internal user `<username>` established.
Applications and Services Logs > Citrix-HostCore-HDX Direct/ Operational	2	HDX Direct	Information	HDX Direct connection for external user `<username>` established.
Applications and Services Logs > Citrix-HostCore-HDX Direct/ Operational	3	HDX Direct	Information	HDX Direct connection for user `<username>` failed.
Applications and Services Logs > Citrix-HostCore-HDX Direct/ Operational	4	HDX Direct	Information	STUN server `<URL:PORT>` provided the following session host IP and PORT mapping for user `<username>`:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOG	ID	SOURCE	LEVEL	DESCRIPTION
				`<IP>:<PORT>` .
Applications and Services Logs > Citrix-HostCore-HDX Direct/ Operational	5	HDX Direct	Information	No response received by session host from any of the configured STUN servers for user `<username>`.
Applications and Services Logs > Citrix-HostCore-HDX Direct/ Operational	6	HDX Direct	Information	Client provided `<IP>:<PORT>` as external mapping for user `<username>`.
Applications and Services Logs > Citrix-HostCore-HDX Direct/ Operational	7	HDX Direct	Information	No external mapping was provided by the client for user `<username>`.

Known issues

HDX Direct might stop working after performing an in-place upgrade of the VDA on a machine that already has **HDX Direct** enabled. To resolve the issue, complete the following steps:

1. Stop the Citrix Certificate Manager Service on the session host.
2. Delete the self-signed Root CA certificate and the self-signed server certificate.
3. Open the registry.
4. Delete the `HKLM\Software\Citrix\HDX-Direct` key.
5. Go to `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Set the **SSLEnabled** value to `0`.
7. Delete the contents of the **SSLThumbprint** value.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Start the **Citrix Certificate Manager Service**.

Secure HDX™

Secure HDX is an Application Level Encryption (ALE) solution that prevents any network elements in the traffic path from being able to inspect the HDX traffic. It does this by providing true End-to-End Encryption (E2EE) at the application level between the Citrix Workspace™ app (client) and the VDA (session host) using AES-256-GCM encryption.

System requirements

The following list depicts the system requirements for using Secure HDX.

- Control plane
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2503 or later
- Session host
  - Operating System
    - Windows 10 22H2
    - Windows 11 22H2 or later
    - Windows Server 2019 or later
  - Virtual Delivery Agent (VDA)
    - Windows: version 2503 or later
    - Linux: version 2407 or later
- Workspace app
  - Windows: version 2503 or later
  - Linux: version 2408 or later
  - Mac: version 2409 or later
  - Chrome OS: version 2409 or later
  - HTML5: version 2408 or later
  - Android: version 2503 or later
  - iOS: version 2503 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Access tier
  - Citrix® StoreFront Cloud
  - Citrix StoreFront 2402 or later

NOTE:

For details on configuring Secure HDX with Linux VDA, refer to the Linux VDA documentation.

Configuration

Secure HDX is disabled by default. You can configure this feature using the Secure HDX setting in Citrix policy:

Secure HDX: Defines whether to enable or disable the feature.

IMPORTANT:

If you have Secure ICA® enabled on the delivery groups that you want to enable Secure HDX on, you must first disable Secure ICA (Edit delivery group > User Settings).

HDX Insight and Smart Control

The following are the requirements to use HDX Insight and SmartControl with NetScaler Gateway when Secure HDX is enabled:

- NetScaler 14.1 Build 47.46 or newer (14.1 Build 72.57 or newer required for EDT support).
- **Network telemetry** must be enabled in Citrix policy. See Network telemetry for details.
- **Session Reliability** must be enabled. This setting is enabled by default, so ensure there are no policies disabling it.

NOTE:

HDX Insight and SmartControl with Secure HDX is available only in the following scenarios:

- When using NetScaler 14.1 Build 47.46 or newer (14.1 Build 72.57 or newer required for EDT)
- Connections using IPv4

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Considerations

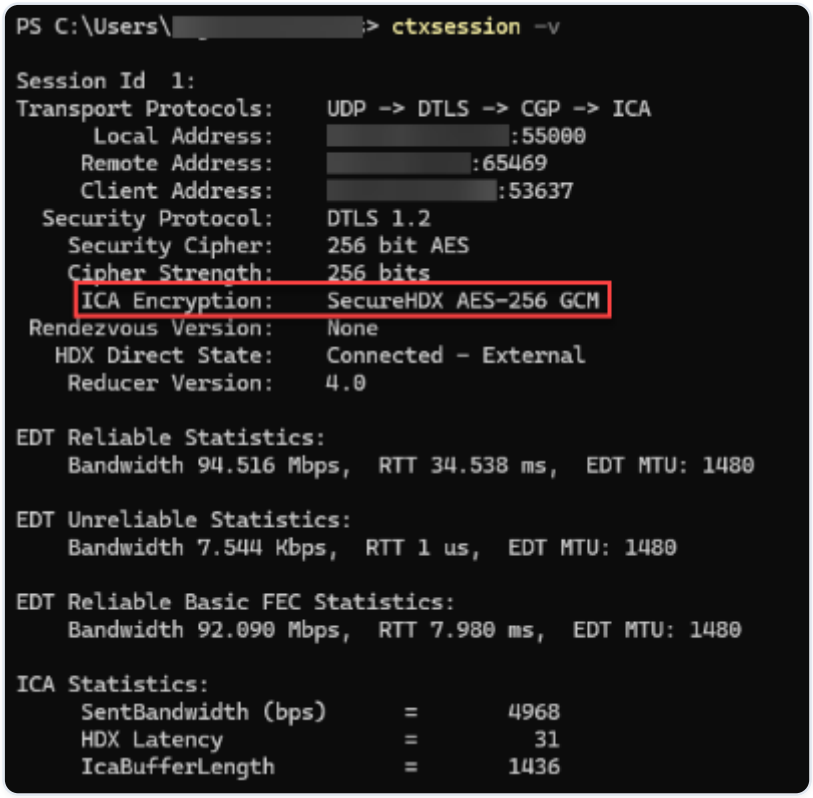
The following are considerations for using Secure HDX:

- If a user tries to connect to a session host with Secure HDX enabled using a client that does not support the feature, the connection will be denied.
- Only Service Continuity for connector-less workloads is supported with Secure HDX. If you are using the standard version of Service Continuity, you will not be able to connect to any session hosts that have Secure HDX enabled if there is a Cloud service outage.
- Multi-Stream ICA is not supported when Secure HDX is enabled.
- If you use any third-party solutions that rely on inspecting HDX traffic, they would no longer work if you enable Secure HDX since HDX traffic is encrypted.

Troubleshooting

To confirm that Secure HDX is active, you can use the `ctxsession.exe` utility on the VDA machine.

To use the `CtxSession.exe` utility, open a Command Prompt or PowerShell within the session and run `ctxsession.exe -v`. If Secure HDX is in use, ICA Encryption displays `SecureHDX AES-256 GCM`.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

When Secure HDX does not get enabled in the session

- Ensure the VDA version in use supports the feature per the system requirements.
- Confirm that you have a policy applied to the VDA that enables Secure HDX and that there are no other policies with higher priority disabling the feature.
- If the session host was already running when you configured Secure HDX, restart the machine to ensure changes take effect.

Network telemetry

Network metrics are critical for Citrix session troubleshooting because the performance and stability of a Citrix session are heavily dependent on the underlying network conditions. Unlike a local application, a Citrix session involves streaming an interactive desktop or application experience over a network, meaning any network instability or bottleneck will directly impact the user's perception of performance.

For details about the network metrics available in Citrix Monitor and Director, see Diagnose Session Performance issues.

System requirements

The following are the system requirements for using Network Telemetry:

- Control plane
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2503 or later
- Virtual Delivery Agent (VDA)
  - Windows: version 2503 or later
  - Linux: version 2507 or later
  - Mac: version 2507 or later
- Workspace app
  - Windows: version 2503 or later
  - Linux: version 2508 or later
  - Mac: version 2505 or later
- Access tier

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix® StoreFront Cloud
- Citrix StoreFront 2402 or later
- Citrix Gateway Service
- Citrix NetScaler Gateway 14.1 Build 47.46 or later (14.1 Build 72.57 or later required for EDT support)

Network requirements

If you are using Citrix Gateway Service, there are no additional network requirements. However, if you are using NetScaler Gateway, there are additional requirements to use Network Telemetry, which are outlined below.

Session hosts

If your session hosts have a firewall such as Windows Defender Firewall, you must allow the following inbound traffic for connections from NetScaler Gateway.

DESCRIPTION	SOURCE	PROTOCOL	PORT
Connection from NetScaler Gateway	NetScaler SNIP	UDP	443
Connection from NetScaler Gateway	NetScaler SNIP	TCP	443

NOTE:

The VDA installer adds the appropriate inbound rules to Windows Defender Firewall. If you use a different firewall, you must add the rules above.

Internal network

The following are the firewall requirements for your internal network:

DESCRIPTION	PROTOCOL	SOURCE	SOURCE PORT	DESTINATION	DESTINATION PORT
Connection from	UDP	NetScaler SNIP	1024-65535	VDA network	443

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DESCRIPTION	PROTOCOL	SOURCE	SOURCE PORT	DESTINATION	DESTINATION PORT
NetScaler Gateway					
Connection from NetScaler Gateway	TCP	NetScaler SNIP	1024-65535	VDA network	443

Configuration

Network telemetry is disabled by default. You can configure this feature via Citrix policy in Studio using the following setting.

- **Network telemetry:** defines whether to enable or disable the feature.

Considerations

The following are considerations for using Network Telemetry:

- To ensure monitoring data remains secure while in transit, connections from NetScaler Gateway to the session hosts are secured with TLS/DTLS when Network Telemetry is enabled. As a result, connections are established on ports UDP 443 (HDX over EDT) and TCP 443 (HDX over TCP) by default. Refer to HDX features managed through the registry if you wish to change the port number.
- Self-managed certificates are used to faciliate network-level encryption for session connections. See HDX Direct certificate management for details on certificate management. Please note that enabling Network Telemetry does not enable HDX Direct.
- Network Telemetry for EDT is supported with NetScaler version **14.1 Build 72.57** and newer. If you are using an older version of NetScaler, sessions will be forced to use TCP if Network Telemetry is enabled.

Virtual channel allow list

The virtual channel allow list is a feature that allows you to control which non-Citrix virtual channels are allowed in your environment. By default, the virtual channel allow list feature is enabled. As a result, only Citrix virtual channels are allowed to open in Citrix Virtual Apps and Desktops™ sessions. If there is a need to use custom virtual channels, whether homegrown or from a third party, these need to be explicitly added to the allow list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration

The virtual channel allow list is enabled by default. You can configure this feature using the following settings in the Citrix policy:

- **Virtual channel allow list**: to enable or disable the feature and to add virtual channels to the list.
- **Virtual channel allow list log throttling**: sets the throttling period for the virtual channel allow list event logging.
- **Virtual channel allow list logging**: sets the logging level for the virtual channel allow list.

Adding virtual channels to the allow list

To add a virtual channel to the allow list, you need the following information:

1. The virtual channel name as defined in the code, which can be up to seven characters long. For example, `CTXCVC1`.
2. The paths to the processes that open the virtual channel on the VDA machine. For example, `C:\Program Files\Application\run.exe`.

Once you have the required information, you must add the virtual channel to the allow list using the Virtual channel allow list policy setting. To add a virtual channel to the list, enter the virtual channel name followed by a comma, and then the path to the process that accesses the virtual channel. If there are multiple processes, you can add these processes by separating each process with commas.

For single processes

Using the previous examples, add the following entry to the list:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

For multiple processes

If there are multiple processes, add the following entry to the list:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using wildcards

The use of wildcards (*) is supported. You can use wildcards when the names of directories or executables change based on the version of the application, or if the third-party component is installed in the users' profiles.

You can use wildcards in the following scenarios:

- To replace the full directory name. For example: `C:\Program Files\Application*\run1.exe`
- To replace part of the directory name. For example: `C:\Program Files\Application\v*\run1.exe`
- To replace the executable's name. For example: `C:\Program Files\Application\v1.2*.exe`
- To replace part of the executable's name. For example: `C:\Program Files\Application\v1.2\run*.exe`

The following restrictions apply:

- The wildcard can only be used to replace a single directory. For example, if the executable is located in `C:\Program Files\Application\v1.2\run1.exe`
  - Allowed: `C:\Program Files\Application*\run1.exe`
  - Not allowed: `C:\Program Files*\run1.exe`
- Entries must contain the file name extension.
  - Allowed: `C:\Program Files\Application\v1.2*.exe`
  - Not allowed: `C:\Program Files\Application\v1.2*`
- All paths must be local.

NOTE:

- Network paths are not allowed.
- Wildcard support is available from Citrix Virtual Apps and Desktops 2206.
- Wildcard support is available in Citrix Virtual Apps and Desktops 2203 LTSR from CU2.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using system environment variables

You can use system environment variables to simplify the definition of the trusted processes in your allow list. You can use any of the out-of-box variables, such as `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%`, and `%systemroot%`.

You can also use custom environment variables as long as they are defined at the system level.

The following examples depict out-of-box environment variables:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

The following example depicts a custom system environment variable:

- Custom variable name: `app`
- Custom variable value: `%programfiles%\Application\`
- Allow list entry: `CTXCVC1,%app%\run.exe`

NOTE:

User environment variables are not supported.

Environment variable support is available from Citrix Virtual Apps and Desktops version 2209.

Obtain virtual channel names and processes

The easiest way to obtain the name of the virtual channel and the process that opens it on the VDA machine is to get the information from the developer or a third-party vendor that provided the virtual channel.

Alternatively, you can obtain information by applying the feature's logs and following these steps:

1. Once the client and server components of the custom virtual channel are in place, launch a virtual application or virtual desktop.
2. In the VDA machine's System event log, look for the custom virtual channel's name and the process that tried to open it. For more information on available events, see Event logs.
3. Log out from the session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Add an entry in the virtual channel allow list policy settings for the identified virtual channel and process.
5. Restart the machine.
6. Once the VDA is registered, run the virtual application or virtual desktop to validate that the custom virtual channels open successfully.

Considerations for Citrix virtual channels

All built-in Citrix virtual channels are trusted and allowed to open without further configuration. However, the following two features require explicit entries in the allow list because of external dependencies:

- Multimedia Redirection
- HDX RealTime Optimization Pack for Skype for Business

Multimedia Redirection

If you use a media player other than Windows Media Player as your system media player, you need to add it to the allow list as a trusted process. The following information is required for the allow list entry:

- Virtual channel name: `CTXMM`
- Process: Path to the media player used in your VDA machine. For example, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Allow list entry: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack for Skype for Business

The following information is required for the allow list entry:

- Virtual channel name: `CTXRMEP`
- Process: Path to the Skype for Business executable in your VDA machine, which can vary based on the version of Skype for Business or if you used a custom installation path. For example, `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`
- Allow list entry: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Considerations for third-party virtual channels

Starting with VDA version 2603, select third-party virtual channels are trusted and allowed to open without further configuration. All other third-party virtual channels require explicit entries in the allow list. The trusted third-party virtual channels are:

- Microsoft Teams
- Zoom Meetings for VDI

IMPORTANT:

The trusted third-party virtual channels are only trusted automatically when the associated applications are installed in their default installation paths. If the applications are installed in a different path, you must explicitly add the virtual channels to the allow list.

Microsoft Teams

The following are the Microsoft Teams virtual channels and the processes' default installation path:

- Virtual channel names: `MSTEAMS`, `MSTEAM1`, and `MSTEAM2`
- Process: `ms-teams.exe`
- Default installation path: `C:\Program Files\WindowsApps\MSTeams.<app version>_x64_8wekyb3d8bbwe\`

Additional information on the Microsoft Teams virtual channels is available in the Microsoft documentation.

Zoom Meetings for VDI

The following are the Zoom Meetings for VDI virtual channels and the processes' default installation path:

- Virtual channel names: `ZOOMHDX`, `ZOOMHDC`, `ZOOMPHX`, `ZOOMCVX`, `ZOOMCCX`, `ZOOMAUS`
- Processes: `Zoom.exe` and `ZoomVDITool.exe`
- Default installation path:
  - 32-bit: `C:\Program Files (x86)\ZoomVDI\bin\`
  - 64-bit: `C:\Program Files\ZoomVDI\bin\`

Additional information on the Zoom Meetings for VDI virtual channels is available in the Zoom documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If your custom virtual channel fails to open, review the following steps:

1. Ensure you are using the correct VDA version.
2. Confirm that you have a policy applied to the VDA with the custom virtual channel in the virtual channel allow list and that there are no other policies with higher priority overwriting this configuration.
3. Check the event log in the VDA and confirm that the virtual channel name reported matches the one defined in the allow list.
    a. If you have multiple processes, ensure these are defined properly as described in Adding virtual channels to the allow list.
    b. If you are using wildcards in the defined process path, ensure you are adhering to the guidelines for Using wildcards.
    c. If you are using environment variables in the defined process path, ensure you are adhering to the guidelines in Using system environment variables.

Event logs

The following events are logged in the VDA machine's event log.

Single-session VDA

The following events are logged in the single-session VDA machine's event log:

LOG NAME	ID	SOURCE	LEVEL	DESCRIPTION
System	2001	`Picadd`	Information	Custom virtual channel `<vcName>` has been opened by process `<processName>`
System	2002	`Picadd`	Warning	Custom virtual channel `<vcName>` cannot be opened by

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOG NAME	ID	SOURCE	LEVEL	DESCRIPTION
				process `<processName>`
System	2003	`Picadd`	Information	`<username>` opened custom virtual channel `<vcName>`
System	2004	`Picadd`	Warning	`<username>` tried to open custom virtual channel `<vcName>`
System	2005	`Picadd`	Error	Path given in policy `<pathInPolicy>` cannot resolve to process path
System	2007	`Picadd`	Information	Loaded process path is `<processPath>`
System	2008	`Picadd`	Error	Environment variable `<varName>` in VC policy path is not found

Multi-session VDA

The following events are logged in the multi-session VDA machine's event log:

LOG NAME	ID	SOURCE	LEVEL	DESCRIPTION
System	13	`Rpm`	Information	Custom virtual channel `<vcName>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOG NAME	ID	SOURCE	LEVEL	DESCRIPTION
				has been opened by process `<processName>`
System	14	`Rpm`	Warning	Custom virtual channel `<vcName>` cannot be opened by process `<processName>`
System	15	`Rpm`	Information	`<username>` opened custom virtual channel `<vcName>`
System	16	`Rpm`	Warning	`<username>` tried to open custom virtual channel `<vcName>`
System	17	`Rpm`	Error	Path given in policy `<pathInPolicy>` cannot resolve to process path
System	18	`Rpm`	Information	Loaded process path is `<processPath>`
System	19	`Rpm`	Error	Environment variable `<varName>` in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LOG NAME	ID	SOURCE	LEVEL	DESCRIPTION
				VC policy path is not found

Known third-party virtual channels

The following are known third-party solutions that use custom Citrix® virtual channels. This list does not include every solution that uses a custom Citrix virtual channel.

- Cerner
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop Software
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Microsoft Teams
- Midmark IQPath Client Extensions
- Nuance PowerMic Client Extensions
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings for VDI
- Ultima IA-Connect

To obtain details for adding the associated virtual channels to the allow list, reach out to the solutions' vendors. Alternatively, follow the steps outlined in the Obtaining virtual channel names and processes section.

Virtual Channel Allow List for DVC

You can use the Virtual channel allow list for DVC to control which custom dynamic virtual channels are allowed in your environment. By default, no dynamic virtual channels are allowed. If there is a need to dynamic virtual channels, these need to be explicitly added to the allow list.

Configuration

The virtual channel allow list for DVC is enabled by default. You can configure this feature using the following setting in the Citrix® policy:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Virtual channel allow list for DVC: to enable or disable the feature and to add dynamic virtual channels to the list.
- Virtual channel allow list log throttling: sets the throttling period for the virtual channel allow list event logging.
- Virtual channel allow list logging: sets the logging level for the virtual channel allow list.

Adding dynamic virtual channels to the allow list

To add a dynamic virtual channel to the allow list, you need the following information:

1. The name of the DVC plug-in on the client. For example, `DvcPlugin1.dll`.
2. The name of the DVC listener(s). For example, `ListenerName1`.
3. The paths to the processes that accesses the dynamic virtual channel on the VDA machine. For example, `C:\Program Files\Application\run.exe`.

Once you have the required information, you must add the dynamic virtual channel to the allow list using the Virtual channel allow for DVC list policy setting. To add a dynamic virtual channel to the list, enter the path to the process that accesses the DVC in the session host followed by a comma, then the client-side plugin name followed by a comma, and the name of the listener used by the plugin. Multiple listener names can be added separated by commas.

For single listener

Using the previous examples, add the following entry to the list: `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1`

For multiple listeners

If there are multiple listeners, add the following entry to the list: `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1,ListenerName2`

Using wildcards

The use of wildcards (*) is supported. You can use wildcards when the names of directories or executables change based on the version of the application, or if the third-party component is installed in the users' profiles.

You can use wildcards in the following scenarios:

- To replace the full directory name. For example: `C:\Program Files\App*\run1.exe`
- To replace part of the directory name. For example: `C:\Program Files\App\v*\run1.exe`
- To replace the executable's name. For example: `C:\Program Files\App\v1.2*.exe`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To replace part of the executable's name. For example: `C:\Program Files\App\v1.2\run*.exe`

The following restrictions apply:

- The wildcard can only be used to replace a single directory. For example, if the executable is located in `C:\Program Files\App\v1.2\run1.exe`
  - Allowed: `C:\Program Files\App*\run1.exe`
  - Not allowed: `C:\Program Files*\run1.exe`
- Entries must contain the file name extension.
  - Allowed: `C:\Program Files\App\v1.2*.exe`
  - Not allowed: `C:\Program Files\App\v1.2*`
- All paths must be local.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Devices

HDX™ provides a high-definition user experience on any device, at any location. The articles in the Devices section describe these devices:

- Client Drive Mapping
- Generic USB device
- Mobile and touch screen devices
- Serial devices
- Specialty keyboards
- TWAIN devices
- Webcams
- WIA devices

Optimized vs. generic USB device

An optimized USB device is one for which Citrix Workspace™ app has specific support. For example, the ability to redirect webcams using the HDX Multimedia virtual channel. A generic device is a USB device for which there is no specific support in Citrix Workspace app.

By default, generic USB redirection can't redirect USB devices with optimized virtual channel support unless put into Generic mode.

In general, you get better performance for USB devices in Optimized mode than in Generic mode. However, there are cases where a USB device doesn't have full functionality in Optimized mode. It might be necessary to switch to Generic mode to gain full access to its features.

With USB mass storage devices, you can use either client drive mapping or generic USB redirection, or both, controlled by Citrix® polices. The main differences are:

If both generic USB redirection and the client drive mapping policies are enabled and a mass storage device is inserted either before or after a session starts, it's redirected using client drive mapping.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When these conditions are true, the mass storage device is redirected using generic USB redirection:

- Both generic USB redirection and the client drive mapping policies are enabled.
- A device is configured for automatic redirection.
- A mass storage device is inserted either before or after a session starts.

For more information, see Configure automatic redirection of USB devices.

FEATURE	CLIENT DRIVE MAPPING	GENERIC USB REDIRECTION
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Encrypted device access	Yes, if encryption is unlocked before the device is accessed on the virtual session.	Citrix Virtual Desktops™ only

Mobile and touch screen devices

Citrix Virtual Apps and Desktops™ enables users to access their published applications and desktops from mobile and touch-screen client devices.

Requirements

Citrix® control plane

- Citrix Virtual Apps and Desktops 7.15 or later
- Citrix DaaS™

Session host

- Operating system
  - Windows 10 1903 or later
  - Windows Server 2016 or later
- VDA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows: version 7.15 or later

Client device

- Operating system
  - Windows 10 1809 or later
- Citrix Workspace™ app for Windows version 1808 or greater

Tablet mode for touch-screen devices using Windows Continuum

Continuum is a Windows 10 feature that adapts to the way the client device is used. When the VDA detects the presence of a keyboard or mouse on a touch-enabled client, it puts the client in to desktop mode. If a keyboard or mouse is not present, the VDA puts the client in to tablet/mobile mode. This detection occurs on session connection and reconnection and also in-session when the keyboard or mouse is attached or detached.

The feature is enabled by default. To disable this feature, configure the policy settings Tablet mode toggle policy settings.

In addition to the requirements for touch screen devices mentioned above, the following are required for Windows Continuum:

XenServer®

- Citrix Hypervisor 8.2 or higher
- Run the XenServer CLI command to allow laptop/tablet switching: **xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1**

IMPORTANT:

Updating the base image for an existing machine catalog after changing the metadata setting doesn't affect any previously provisioned VMs. After changing the XenServer VM base image, create a catalog, choose the base image, and provision a new Machine Creation Services™ (MCS) machine.

Session host

- Operating system
  - Windows 10 1903 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Windows 11

- VDA

    - Windows: version 7.16 or later
    - **Due to current limtations in the Operating system configurations, the user will have to set the following options from the drop-down menus after they start the first ICA® session and restart the VDA:**

        - **Settings > System > Tablet Mode**

            - Use the appropriate mode for my hardware
            - Don’t ask me and always switch



The **tablet mode** offers a user interface that is better suited to touch screens:

- Slightly larger buttons
- The Start screen and any apps you start open in a full screen
- The Taskbar contains a back button
- Icons deleted from the task bar

You have access to the File Explorer.



Windows 10 loads the GPIO driver on the target virtual machine based on this updated BIOS. It is used for toggling between tablet and desktop modes within the virtual machine.

Citrix Workspace app for HTML5 does not support Windows Continuum features.

The **desktop mode** offers the traditional user interface where you interact in the same manner as using a PC and a keyboard and mouse.

Microsoft Surface Pro and Surface Book pens

We support standard pen functionality with Windows Ink-based applications. Support includes pointing, erasing, pen pressure, Bluetooth signals, and other features depending on the operating system firmware and pen model. For example, pen pressure can be up to 4096 levels. This feature is enabled by default.

The following are the requirements for pen functionality support:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix control plane

- Citrix Virtual Apps and Desktops 1903 or later
- Citrix DaaS

Session host

- Operating system
  - Windows 10 1809 or later
  - Windows Server 2016 or later
  - Windows 11
- VDA
  - Windows: version 1903 or later

Client device

- Operating system
  - Windows 10 1809 or later
- Citrix Workspace app for Windows minimum version 1902

For a demonstration of Windows Ink and the pen functionality, click this graphic:



To disable or enable this feature, see Microsoft Surface Pro and Surface Book pens in the list of features managed through the registry.

Known issues

The following are known issues with Pen support:

- Due to OS limitations in Windows server 2k22, users will not be able to set pen shortcuts or make adjustments to pen/ink settings in the Control Panel when connecting to 2k22 server applications or desktops.
- Pen shortcuts are not being honored from a pen enabled Windows 11 client due to OS limitation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Serial devices

Most new PCs don't have built-in serial (COM) ports. The ports are easy to add by using USB converters. Applications suited for serial ports often involve sensors, controllers, old check readers, pads, and so forth. Some USB virtual COM-port devices use vendor-specific drivers in place of the Windows-provided drivers (usbser.sys). These drivers allow you to force the virtual COM port of the USB device so that it doesn't change even if connected to different USB sockets. This might be done from the **Device Manager > Ports (COM & LPT) > Properties** or from the application that controls the device.

Client COM port mapping allows devices attached to the COM ports on the user's endpoint to be used during virtual sessions. You can use these mappings like any other network mappings.

For each COM port, a driver in the operating system assigns a symbolic link name such as COM1 and COM2. The applications then use the link to access the port.

IMPORTANT:

Because a device can attach to the endpoint by using USB directly, doesn't mean it can be redirected using generic USB redirection. Some USB devices function as virtual COM ports, which applications can access in the same way as physical serial port. The operating system can abstract COM ports and treat them like fileshares. Two common protocols for virtual COM are CDC ACM or MCT. When connected through an RS-485 port, applications might not work at all. Get an RS-485-to-RS232 converter to use RS-485 as a COM port. **Important:**

Some applications recognize the device (for example, a signature pad) consistently only if it is connected to COM1 or COM2 on the client workstation.

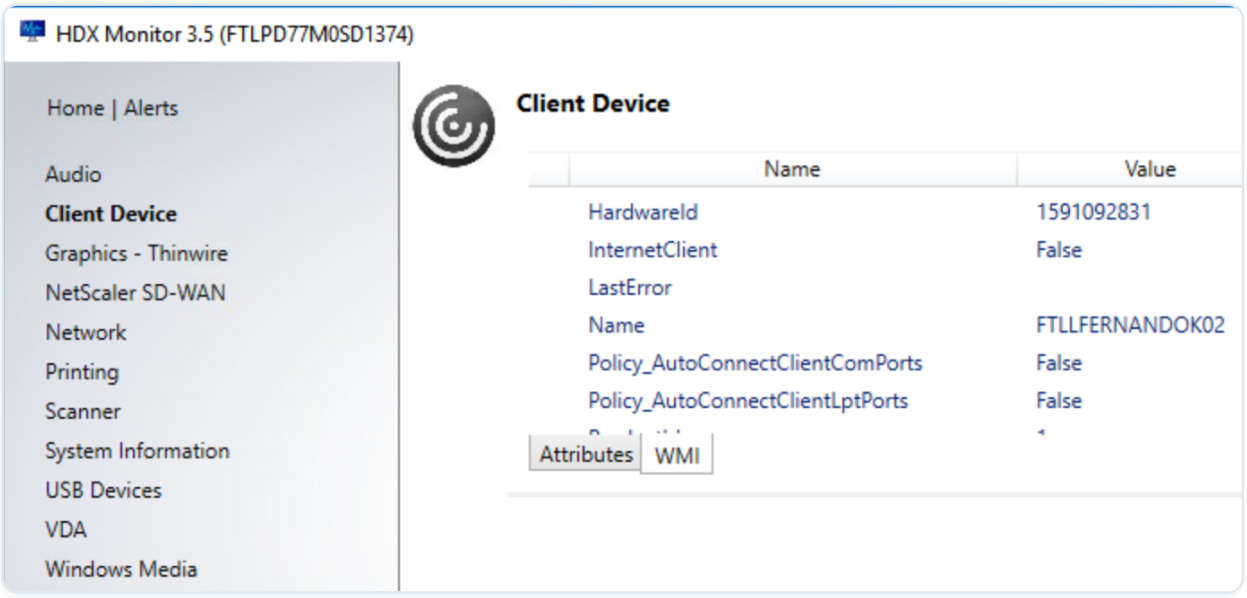
Map a client COM port to a server COM port

You can map client COM ports to a Citrix® session in three ways:

- Studio policies. For more information about policies, see Port redirection policy settings.
- VDA command prompt.
- Remote Desktop (Terminal Services) configuration tool.

1. Enable the **Client COM port redirection** and the **Auto connect client COM ports Studio** policies. After applied, some information is available in HDX™ Monitor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. If **Auto connect client COM ports** failed to map the port, you can map the port manually or use logon scripts. Log on to the VDA, and at a command prompt window, type:

   NET USE COMX: \\\CLIENT\COMZ:

   Or

   NET USE COMX: \\\CLIENT\\CLIENTPORT:COMZ:

   X is the number of the COM port on the VDA (ports 1 through 9 are available for mapping). **Z** is the number of the client COM port you want to map.

   To confirm that the operation was successful, type **NET USE** at a VDA command prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports.



3. To use this COM port in a virtual desktop or application, install your user device application and point it to the mapped COM port name. For example, if you map COM1 on the client to COM3 on the server, install your COM port device application in the VDA and point it to COM3 during the session. Use this mapped COM port as you would a COM port on the user device.

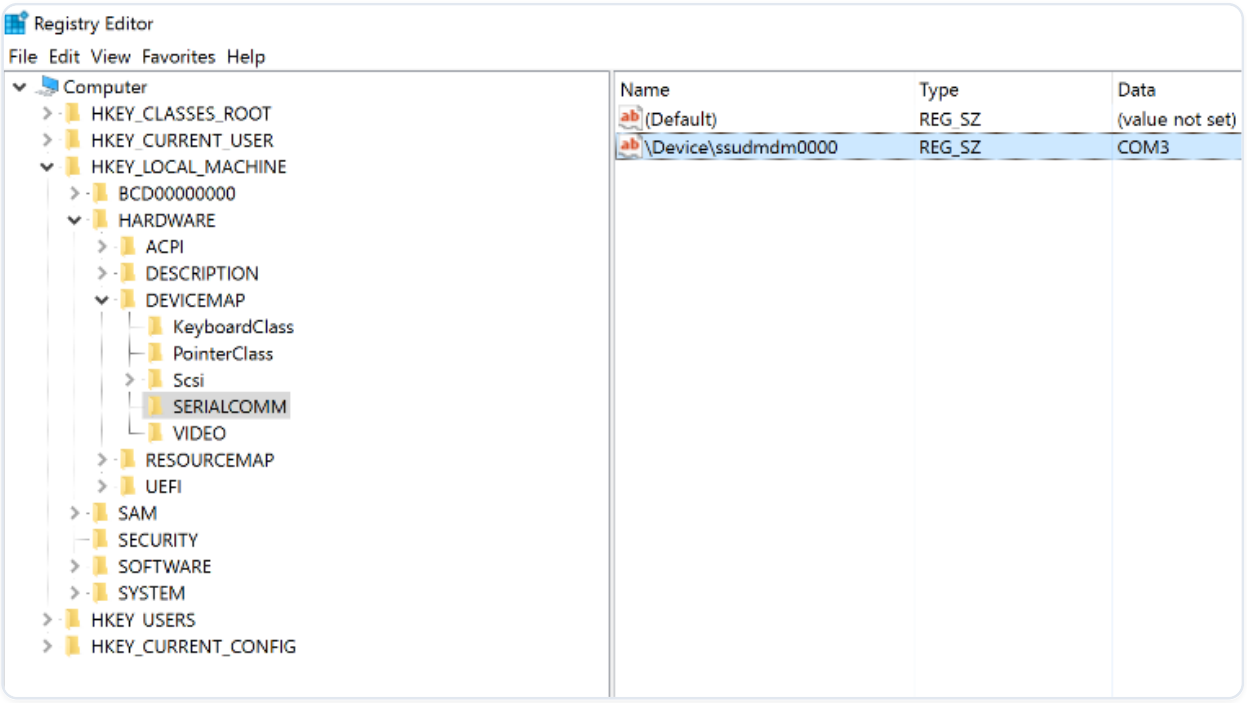
© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

COM port mapping is not TAPI-compatible. You can't map Windows Telephony Application Programming Interface (TAPI) devices to client COM ports. TAPI defines a standard way for applications to control telephone functions for data, fax, and voice calls. TAPI manages signaling, including dialing, answering, and ending calls. Also, supplemental services such as holding, transferring, and conference calls.

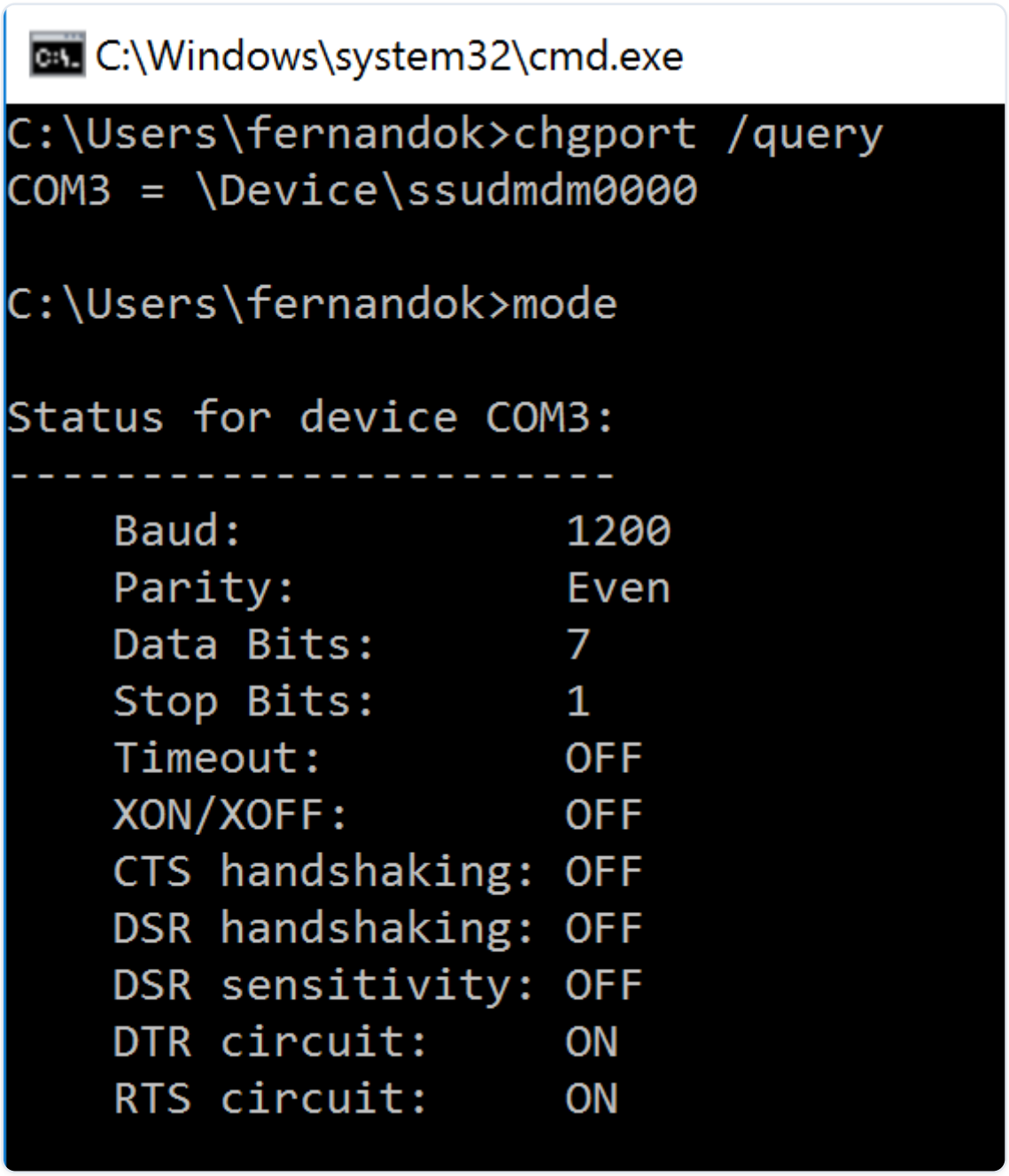
Troubleshoot

1. Ensure you can access the device directly from the endpoint, bypassing Citrix. While the port is not mapped to the VDA, you are not connected to a Citrix session. Follow any troubleshooting instructions that came with the device and verify that it works locally first. When a device is connected to a serial COM port, a registry key is created on the hive shown here:



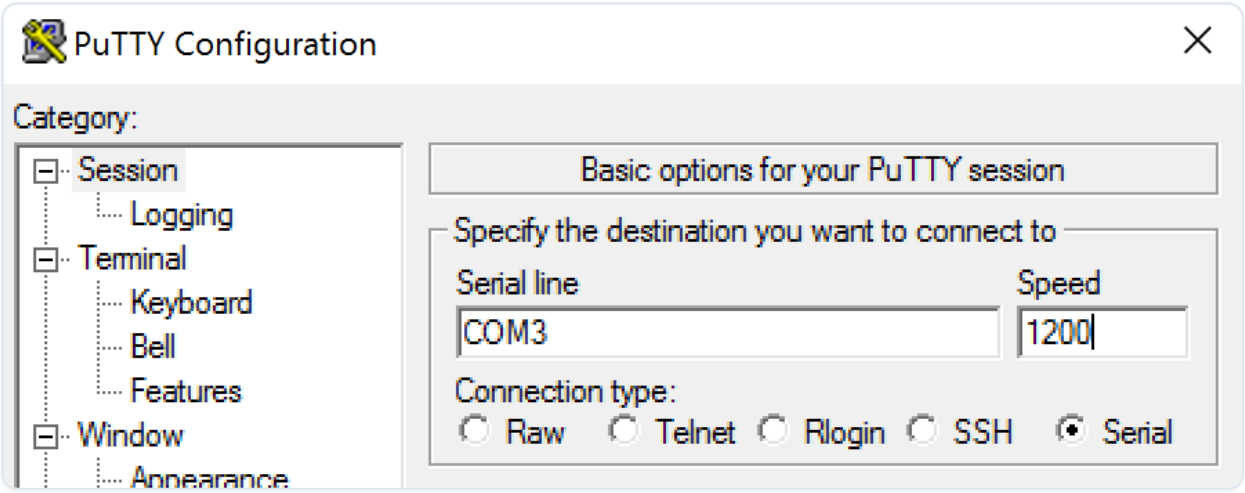
   You can also find this information from the command prompt by running **chgport /query**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If troubleshooting instructions for the device aren't available, try opening a PuTTY session.

Choose **Session** and in **Serial line** specify your COM Port.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can run **MODE** in a local command window. The output might display the COM port in use and the Baud/Parity/Data Bits/Stop Bits, which you need in your PuTTY session. If the PuTTY connection is successful, press **Enter** to see feedback from the device. Whatever characters you type might be repeated on the screen, or responded to. If this step is unsuccessful, you can't access the device from a virtual session.

2. Map the local COM port to the VDA (using policies or **NET USE COMX: \\\CLIENT\COMZ:**) and repeat the same PuTTY procedures in the previous step, but this time from the VDA PuTTY. If PuTTY fails to show the error **Unable to open connection to COM1. Unable to open serial port**, another device might be using COM1.
3. Run **chgport /query**. If the built-in Windows serial driver on the VDA is auto-assigning \Device\Serial0 to a COM1 port of your VDA, do the following: A. Open CMD on the VDA and type **NET USE.**

   B. Delete any existing mapping (for example, COM1) on the VDA.

   NET USE COM1 /DELETE

   C. Map the device to the VDA.

   NET USE COM1: \\\CLIENT\COM3:

   D. Point your application on the VDA to COM3.

   Lastly, try to map your local COM port (for example, COM3) to a different COM port on the VDA (other than COM1, for example COM3). Ensure that your application is pointing to it: **NET USE COM3: \\\CLIENT\COM3**
4. If now you do see the port mapped, PuTTY is working but no data passing, it might be a race condition. The application might connect and open the port before it is mapped, locking it from being mapped. Try one of the following:

   - Open a second application published on the same server. Wait a few seconds for the port to be mapped, and then open the real application that tries to use the port.
   - Enable the COM port redirection policies from the Group Policy Editor in Active Directory instead of Studio. Those policies are **Client COM port redirection** and **Auto connect client COM ports**. Policies applied this way might be processed before the Studio policies, guaranteeing that the COM port is mapped. Citrix policies are pushed to the VDA and stored in: `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Use this logon script for the user or instead of publishing the application, publish a .bat script that first deletes any mapping on the VDA, remaps the virtual COM port, and then starts the application:

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: \\ \CLIENT\COM1: NET USE COM2: \\\CLIENT\COM2: MODE COM1: BAUD=1200 (or whatever value needed) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (or whatever value needed) START C:\\Program Files\\\<Your Software Path>\\\<your_software.exe>

5. Process Monitor from Sysinternals is the tool of last resort. When running the tool on the VDA, find and filter objects like COM3, picaser.sys, CdmRedirector, but especially \<your_app\>.exe. Any errors might appear as Access Denied or similar.

Specialty keyboards

Bloomberg keyboards

WARNING:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Citrix Virtual Apps and Desktops™ support the Bloomberg model 4 Starboard keyboard (and earlier model 3). This keyboard enables customers in the financial sector to use the special features of the keyboard to access financial market data and perform trading quickly.

This keyboard is compatible with the KVM switch boxes and can work in two modes:

- PC (One USB cable with no KVM)
- KVM mode (Two USB Cables with one routed through KVM)

IMPORTANT:

We recommend that you use the Bloomberg keyboard with only one session. We don't recommend using the keyboard with multiple concurrent sessions (one client to multiple sessions).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Bloomberg keyboard 4 is a USB composite device comprising four USB devices in one physical shell:

- Keyboard.
- Fingerprint reader.
- Audio device with keys to increase and decrease volume and mute the speaker and the microphone. This device includes onboard speaker, microphone, and jack for the microphone and headset.
- USB hub to connect all of these devices to the system.

Requirements:

- The session to which Citrix Workspace™ app for Windows is connecting must support USB devices.
- Minimum of Citrix Workspace app 1808 for Windows or Citrix Receiver for Windows 4.8 to support Bloomberg keyboard model 3 and 4.
- Minimum of Citrix Workspace app 1808 for Windows or Citrix Receiver for Windows 4.12 to use KVM mode (two USB cables with one routed through KVM) for Model 4.

For information about configuring Bloomberg keyboards on Citrix Workspace app for Windows, see Configuring Bloomberg keyboards.

To enable Bloomberg keyboard support, see Bloomberg keyboards in the list of features managed through the registry.

Verify support:

To determine if Bloomberg keyboard support is enabled in Citrix Workspace app, check if the Desktop Viewer correctly reports the Bloomberg keyboard's devices.

Desktop scenario:

Open the Desktop Viewer. If support for Bloomberg keyboard is enabled, the Desktop Viewer shows see three devices under the USB icon:

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

Seamless Application only scenario:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Open the **Connection Center** menu from the Citrix Workspace app notification area icon. If support for the Bloomberg keyboard is enabled, the three devices appear in the **Devices** menu.

The check mark against each of these devices indicates that they are remoted to the session.

Webcams

High definition webcam streaming

Webcams can be used by video conferencing applications running within the virtual session. The application on the server selects the webcam format and resolution based on the supported format types. When a session starts, the client sends the webcam information to the server. Choose a webcam from the video conferencing application. When the webcam and the application both support high-definition rendering, the application uses high-definition resolution. We support webcam resolutions up to 1920x1080.

This feature requires the Citrix Receiver for Windows, minimum version 4.10. For a list of Citrix Workspace app platforms that support HDX webcam redirection, see Citrix Workspace app feature matrix.

For more information about high-definition webcam streaming, see HDX video conferencing and webcam video compression.

You can use a registry key to disable and enable the feature and then configure a specific resolution. For information, see High-definition webcam streaming and High-definition webcam resolution in the list of features managed through the registry.

Scanning

Scanner is a device that optically scans images, printed text, handwriting or an object and converts it to a digital image.

If you’re using a scanner and your computer is running windows, there’s a good chance you’re using the WIA scanner driver. This driver is responsible for communicating between your computer and scanner.

- **Windows Image Acquisition** (WIA) is Microsoft’s driver model and application programming interface (API) that enables software to communicate with imaging hardware like scanners.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **TWAIN** (Windows and Mac) is another protocol which is a scanning protocol that connects scanners and applications together by providing standard interface. TWAIN allows applications to acquire images from TWAIN compliant devices (scanners, digital cameras, etc.).

TWAIN Redirection

Introduction

TWAIN is a scanning protocol used to link image software to scanners or digital cameras.

How TWAIN works

- Scan your documents using any of the 32-bit applications in your Citrix® session.

> **NOTE:**
>
> Use a locally attached TWAIN-compliant scanner to scan the documents.

- The Citrix scanning module redirects the TWAIN request to the client's scanner.
- Once the scan is complete, the session host is notified.

Requirements

Citrix Control Plane

- Citrix Virtual Apps and Desktops™ 1912 or later
- Citrix DaaS™

Session Host

- Operating system
  - Windows 10 1809 or later
  - Windows 11
  - Windows Server 2022 or later
- VDA
  - Version 1912 or later
- Application
  - 32-bit application

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client Device

- Operating system
  - Windows 10 1809 or later
  - Windows 11
- Workspace app
  - Windows: version 1912 or later
- Scanner
  - TWAIN-compliant scanner

Configuration

- Install TWAIN drivers on the client endpoint.
- Set up devices or applications to select the required scanning protocol if they support both TWAIN and WIA.
- Attach the scanner to the client endpoint locally (through USB).
- Redirect TWAIN devices to the session via USB redirection if needed.

> **NOTE:**
>
> TWAIN devices don't work well with USB redirection leading to poor scan quality.

Policy Settings

Policy settings to set up TWAIN redirection and improve scanning.

- **Client TWAIN device redirection:** to enable or disable TWAIN redirection.

> **NOTE:**
>
> By default, TWAIN redirection is enabled.

- **TWAIN compression level:** to set compression levels for images from client to host.

For more details, see TWAIN devices policy settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

Try out TWAIN with the public test app Twacker, which can be downloaded from this URL.

Follow the steps to validate TWAIN within a published desktop session:

1. Install **Twacker** on the VDA.
2. Launch **Twacker** (32-bit version).
3. Click **File > Select Source** and select your scanner from the list.
4. Click **File > Acquire**.
5. Click the **Scan button** to test your scanner.

If **Twacker** can scan successfully, it confirms that the **Citrix Virtual Apps and Desktops** setup is:

- Configured for USB redirection
- Using TWAIN devices
- Meeting all local client device requirements

If you still have scanning issues within a particular application, then it's likely to be a software issue.

WIA Devices

Requirements

- The scanner must be WIA compliant.
- Install the WIA drivers on the local device. They are not required on the server.
- Attach the scanner locally (for example, through USB).
- Ensure that the scanner is using the local Windows Image Acquisition service and not the TWAIN driver.
- Ensure that there is no policy applied to the user account that is used for the test, and which is limiting the bandwidth within the ICA® session. For example, client USB redirection bandwidth limit.

Windows Image Acquisition application allow list

An allow list lets you control which applications on the VDA can access the Windows Image Acquisition scanner redirection. The Registry Editor uses input from the allow list setting on each

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA that contains Windows Image Acquisition. By default, no applications have access to Windows Image Acquisition.

To adjust Windows Image Acquisition for applications on the VDA, see the Windows Image Acquisition application allow list setting in the list of features managed through the registry.

For information about policy settings, see WIA devices policy settings.

USB Devices

HDX™ technology provides **optimized support** for most popular USB devices. These devices include:

- Monitors
- Mice
- Keyboards
- Voice over Internet Protocol phones
- Headsets
- Webcams
- Scanners
- Cameras
- Printers
- Drives
- Smart card readers
- Drawing tablets
- Signature pads

Optimized support offers an improved user experience with better performance and bandwidth efficiency over a WAN. Optimized support is usually the best option, especially in high latency or security-sensitive environments.

HDX technology provides **generic USB redirection** for specialty devices that don't have optimized support or where it is unsuitable. For more information about generic USB redirection, see Generic USB redirection.

For more information about USB devices and Citrix Workspace app for Windows, see Configuring composite USB device redirection and Configuring USB support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration

USB redirection is disabled by default. You can configure generic USB redirection using the following settings in Citrix® policy:

- **Client USB device redirection**: to enable or disable USB redirection
- **Client USB device redirection rules**: to specify specific device action i.e. to allow or deny access to a particular device
- **Client USB device redirection rules (Version 2)**: to specify rules for filtering, splitting and auto-connecting USB devices
- **Client USB device optimization rules**: to disable optimization or change the optimization mode
- **Allow existing USB devices to be automatically connected**: to allow or prevent automatic connection of existing USB devices that are connected to a client endpoint at the start of an HDX™ session
- **Allow newly arrived USB devices to be automatically detected**: to allow or prevent automatic connection of USB devices that are connected to a client endpoint during an HDX session

See, USB Policy Settings for more details.

How to configure USB redirection

By default, USB redirection configuration is disabled. To use it, USB redirection policy and specific redirection rules must be enabled and configured on the DDC.

NOTE:

If you are using any components older than version 2212 or you are using Workspace App for Linux/Mac, see Legacy USB Redirection Configuration for details on how to configure USB redirection.

Enabling Generic USB Redirection

1. Open **Citrix Web Studio™ policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA® > USB Devices policies**.
3. Edit the **Client USB device redirection policy**.
4. Select **Allowed** and click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Creating USB Redirection Policy Rules

When the user tries to redirect a USB device to Virtual Desktop, it is checked against each USB policy rule in turn until a match is found. The first match for any devices is considered final. If the first match is an **Allow** rule, the matched device is allowed to be redirected to the virtual desktop. If the first match is a **Deny** rule, the matched device is only available in the local desktop. If no match is found, default rules are used.

DEVICE RULES

As with regular USB devices, device rules set in the policy or client Citrix Workspace™ app configuration on the end point select the devices for forwarding. Citrix Workspace app uses these rules to decide which USB devices to allow or prevent from forwarding to the remote session.

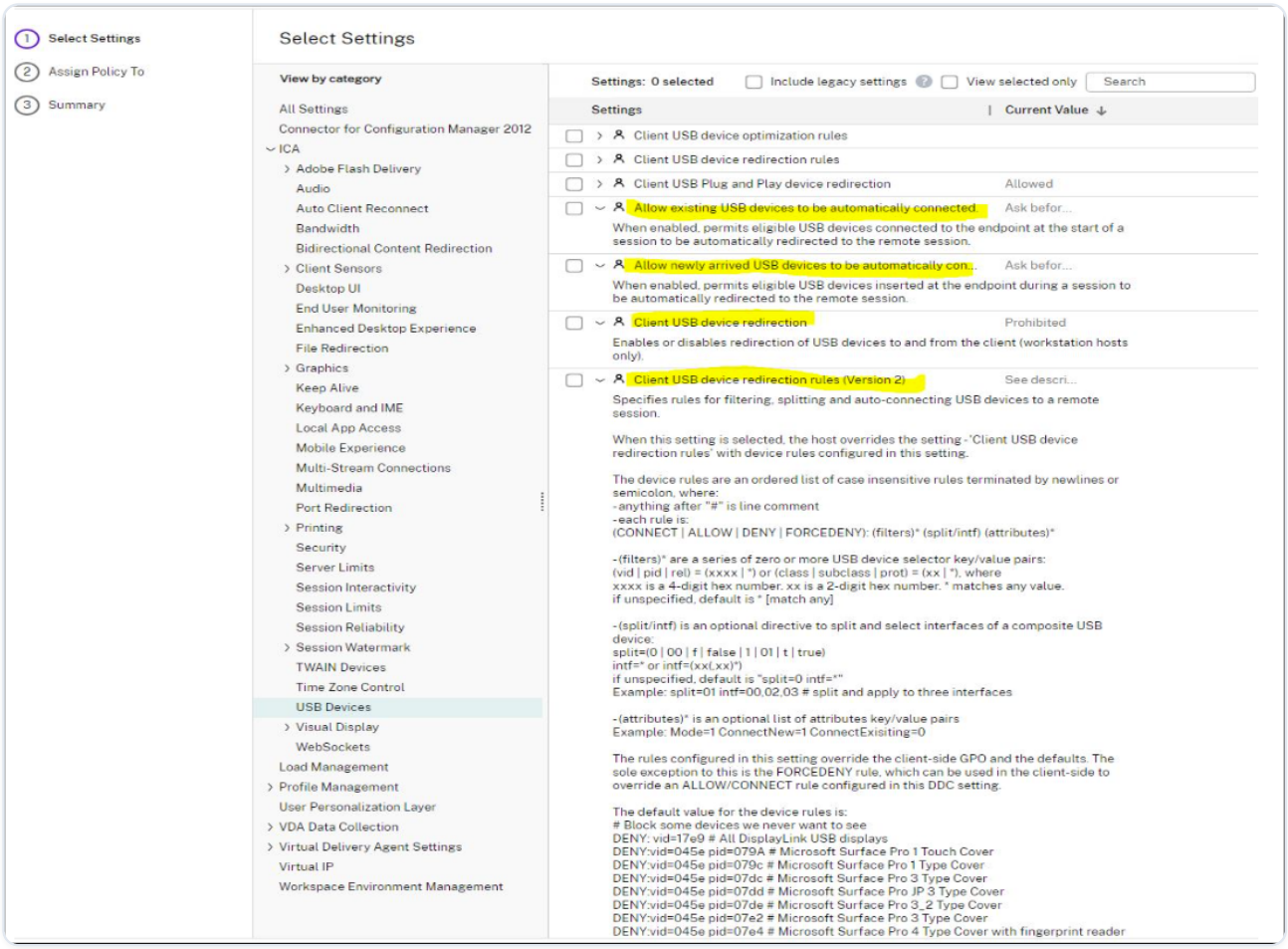
Each rule consists of an action keyword (**Allow, Connect, or Deny**), a colon (:), and zero or more filter parameters that match actual devices at the endpoints USB subsystem. These filter parameters correspond to the USB device descriptor metadata used by every USB device to identify itself.

Device rules are clear text with each rule on a single line and an optional comment after a # character. Rules are matched top down (descending priority order). The first rule that matches the device or child interface is applied. Subsequent rules that select the same device or interface are ignored.

Example: ALLOW VID=1050 PID=0421 #Device1 **Example:** CONNECT VID=xxxx PID=yyyy Class=03 #Device2

KEYWORD	DESCRIPTION
CONNECT	Use this keyword to allow devices to be redirected over the USB virtual channel as well as enable them to be auto-redirected during session launch and upon insertion.
ALLOW	Use this keyword to allow devices to be redirected over the USB virtual channel
DENY	Use this keyword to deny devices from being redirected over the USB virtual channel

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Setting the policy on the DDC:

1. Open **Citrix Web Studio policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA > USB Devices policies**.
3. Edit the **Client USB device redirection rules** (**Version 2**).
4. Set the value based on the examples provided in the description for each usb device that needs to be redirected and click Save.

   For Example: Allow: VID=056A PID=00A4 #STU-430 Deny: Class=08 subclass=05 # Mass Storage

   NOTE:

   If a Citrix admin checks **Use default value** and clicks on **Save**, the default rules can be found in the following registry in the VDA.

   Caution!

   Refer to the Disclaimer at the end of this article before using the Registry Editor.

   `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Policies can still be set on the client device using group policy device rules but that is no longer needed on newer versions of CVAD and CWA.

For legacy configuration of USB devices, see Legacy USB Redirection Configuration.

Configure automatic redirection of USB devices (Optional)

USB devices are automatically redirected when USB support is enabled. Also, the USB user preference settings are set to automatically connect USB devices. It is not always best to redirect all USB devices. Users can explicitly redirect devices from the USB device list that are not automatically redirected. To prevent USB devices from being listed or redirected, use DeviceRules on either the client endpoint or the DDC policy. This policy can be set either on the DDC, on the client using a GPO, using Citrix Workspace app Preferences or the Connections tab under CDViewer. All of these methods are described below:

Setting the policy on the DDC:

There are two policies on the DDC that can be set to allow auto redirection of USB devices-

- Allow existing USB devices to be automatically connected
- Allow newly arrived USB devices to be automatically connected

a. Open **Citrix Web Studio policies** and click on the **Policies** tab.

b. Click on **Create Policy** and expand the **ICA > USB Devices policies**.

c. Edit the setting **Allow** existing USB devices to be automatically connected.

d. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

e. Edit the setting **Allow** newly arrived USB devices to be automatically connected.

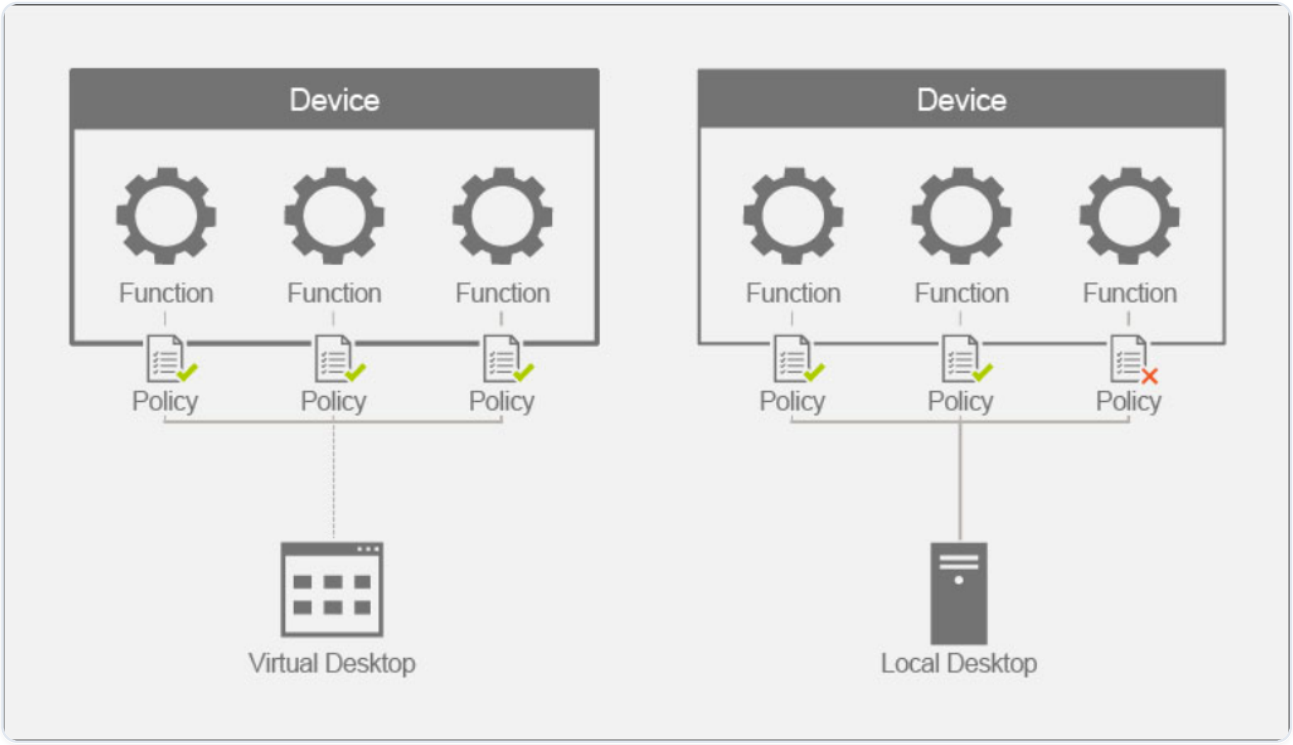
f. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Composite Devices and Device Splitting

A composite USB device is a single device that acts like multiple independent USB devices connected to a computer. It has a single USB connector but it can expose multiple interfaces to the computer with each having its own set of functionalities. When a user plugs in a composite USB device, the host device checks for all functions (interfaces) against each policy rule. If the first

© 1997–2026 Citrix Systems, Inc. All rights reserved.

match for any function(interface) is a Deny rule, the rule is considered definitive for the composite device and the device is denied. If the first match for a function (interface) is an Allow rule, the host device continues to match the rules against the next function (interface). The composite device is allowed if no function (interface) is denied by a policy rule. If definitive match for composite device is a Deny Rule, the device is available only to the local desktop otherwise the device is remoted to the virtual desktop. If no match is found, default rules are used.



We can split the composite device using the appropriate rules in the Device redirection rules (Version 2) policy to allow only specific functionality of a composite device. For instance, we may want to use just the HID functions of a FIDO2 key but not the smartcard functionality. In that case, we would set the rules as illustrated below:

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey series 5 allowed FIDO2 HID functions.
2. Deny: VID=1050 PID=0407 split=01 intf=02 # Yubikey series 5 smartcard function blocked.

TIP:

When creating new policy rules, refer to the USB Class Codes, available on the USB web site.

Configuring a signature pad

1. Install the appropriate device driver on the VDA host.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Turn On the **Client USB device redirection policy** in **Citrix Web Studio™**.
3. Edit the **Client USB device redirection rules** (**Version 2**) policy.
    a. Set the **VID** and **PID** information for the signature pad that needs to be redirected and click **Save**. For example: **Connect**: VID=056A PID=00A4 #STU-430
4. Edit the policy **Client USB device optimization rules**.
    a. Set the mode along with other device information. For example: Mode=00000004 VID=056A PID=00A4 class=03 #Input device operating in capture mode
5. Edit the policy **Allow existing USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
7. Edit the policy **Allow newly arrived USB devices to be automatically connected**.
8. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Once these policies are set in the Studio console, subsequent session launches will have the device getting automatically redirected and will not require any additional end user action.

NOTE:

Replace the VID and PID with the actual VID and PID of the device to be redirected.

Configuring Bloomberg keyboard using USB redirection

1. Turn On the **Client USB device redirection policy** in **Citrix Web Studio**.
2. Bloomberg 5 keyboards are set by default in the Client USB device redirection rules (Version 2) policy and no additional admin action is needed.
3. Edit the policy **Allow existing USB devices to be automatically connected**.
4. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
5. Edit the policy **Allow newly arrived USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Once these policies are set in the Studio console, Bloomberg keys will automatically be presented in subsequent HDX™ sessions and will not require any additional end user action.

Configuring a FIDO2 key using USB redirection

Citrix recommends using FIDO2 redirection for using FIDO2 keys in your HDX sessions. However, there might be situations in which you must redirect FIDO2 keys using USB redirection instead. These include scenarios where FIDO2 redirection is not available because the feature is not supported by the client, the VDA, or the operating system (e.g. Windows Server 2016).

There can also be situations in which the key has multiple modes enabled, but you only want to allow a subset of those in your HDX sessions. For example, you might want to allow FIDO2 and OTP, but block the smart card.

The following steps illustrate how you can configure a FIDO2 key using USB redirection (Yubikey vid=1050, pid=0407).

1. turn On the **Client USB device redirection policy** in **Citrix Web Studio**.
2. Edit the **Client USB device redirection rules** (Version 2) policy.
    a. Set the **VID** and **PID** information as well as the split device configuration for the FIDO2 key to be redirected in the session and click **Save**.
    b. **Connect**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey series 5 allowed FIDO2 HID functions.
    c. **Deny**: VID=1050 PID=0407 split=01 intf=02 # Yubikey series 5 smartcard function blocked.
3. Edit the policy **Allow existing USB devices to be automatically connected**.
4. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
5. Edit the policy **Allow newly arrived USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Once these policies are set in the Studio console, FIDO2 keyboards will automatically be presented in subsequent HDX sessions and will not require any additional end user action.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring a 3-d mouse using USB redirection

Today, the 3dConnexion space mouse drivers are only supported on workstation OSes (Win 10 and Win11). They do not work on server OS. The following are the steps to configure a SpaceMouse Enterprise on a workstation OS (vid=046D, pid=C016).

1. Install the latest Windows driver on the VDA host.
2. From Studio, turn on **Client USB device redirection policy**.
3. Edit the **Client USB device redirection rules** (**Version 2**) policy.
    a. Set the **VID** and **PID** information for the signature pad that needs to be redirected and click **Save**. For example: **Connect**: VID=046D PID=C016 #SpaceMouse Enterprise
4. Edit the policy **Client USB device optimization rules**.
    a. Set the mode along with other device information. For example: Mode=00000004 VID=046D PID=C016 class=03 #Input device operating in capture mode
5. Edit the policy **Allow existing USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
7. Edit the policy **Allow newly arrived USB devices to be automatically connected**.
8. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Troubleshooting

The following steps should be followed to triage USB redirection related issues:

1. Validate system requirements are being met for USB redirection. This includes correct CVAD and CWA versions, supported devices and device drivers on the OS platform under consideration.
2. Ensure the configuration is appropriate based on the components' versions and platforms in use in your environment. See the note in Legacy USB Redirection Configuration for details on components that require legacy configuration settings.
3. Validate that device is listed under devices that the client has enumerated.
    a. Workspace Preferences toolbar: Look at the devices enumerated in the Devices tab of the Workspace app Preferences toolbar (Right click **CWA icon > Connection Center > Preferences**… Click on **Devices** tab).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. `CtxUsbDiagnostics.exe` (Recommended): Run this tool in a command prompt window. The output gives you device specific information for a specific session. It will tell you if a device is being redirected or not. It will also tell you if a device rule set is causing the device to not be redirected. See, Diagnostics Tool for more information.

c. USBView or other 3rd party tools: Run a 3rd party tool like USBView in the endpoint / client machine to ensure that the device is detected at the endpoint.

4. If you see the device being enumerated:

   a. If you see a Deny rule in the CtxUsbDiagnostics tool output for a particular device, check the policies configured in Studio and ensure that the rules are correctly set in Version 2 policy. If the deny rule doesn't appear in the studio policy, check the client side policy and finally the client side defaults in that order to find the matching deny rule.

   b. If there is no deny rule in the CtxUsbDiagnostics output, then CWA will allow redirection of the device by checking / clicking the appropriate button in the devices tab of the Preferences window (Devices > Manage devices). A device once redirected will be available in the session. This can be verified by checking the device manager / USBView or similar application in the HDX session.

5. If you do not see the device being presented inside the session:

   a. It is possible that the correct device driver is not installed correctly on the VDA host. Ensure that the latest versions of device drivers are correctly installed on the VDA host. Some device drivers are not supported on terminal server machines so ensure that is not the case with the device you are trying to redirect.

   b. Ensure that the device is not being used on the client endpoint. Some devices require drivers to be installed on the client endpoint as well and this could prevent them from being redirected in the session.

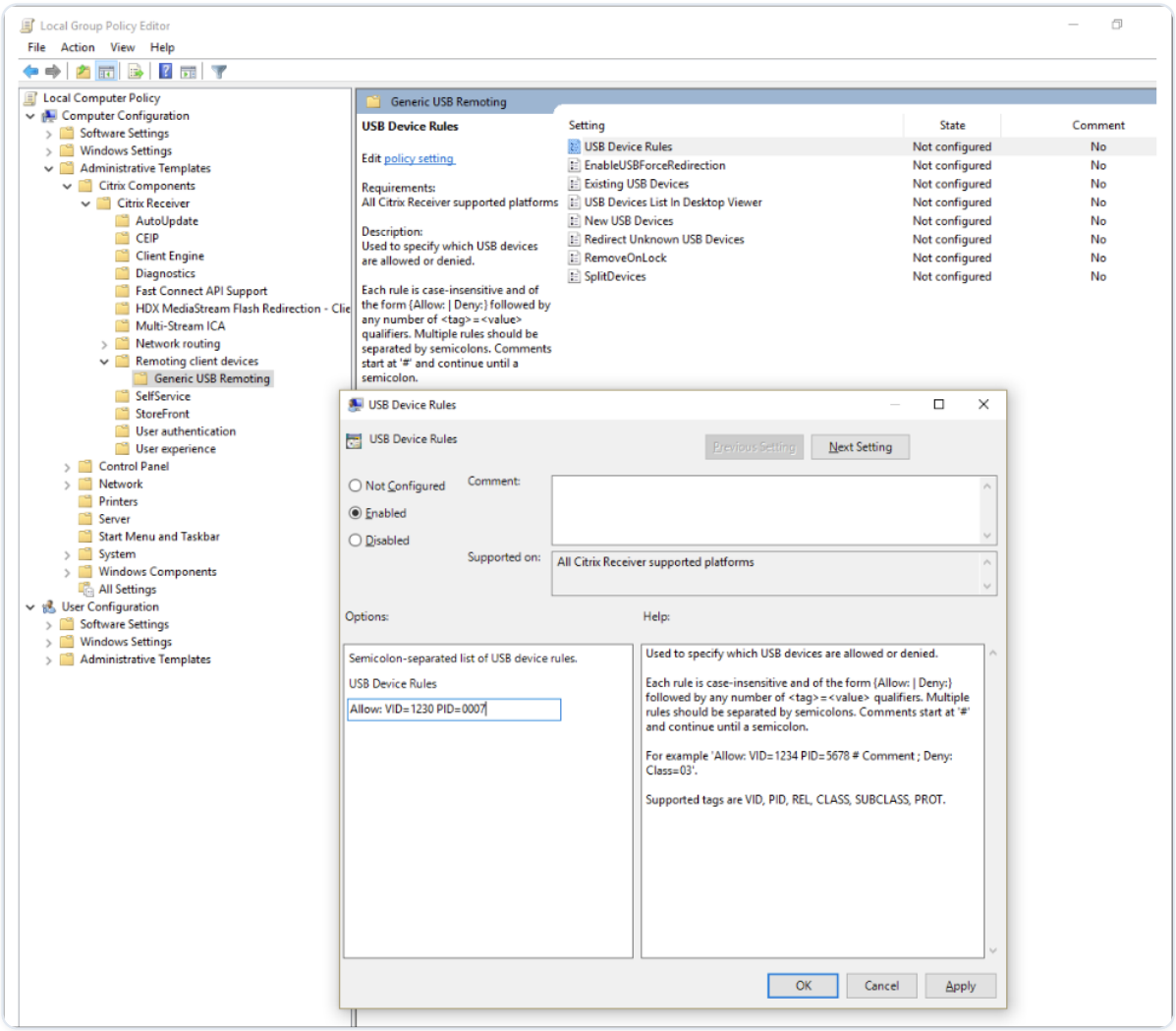
6. Validate USB related rules are set correctly on the client endpoint:

   a. **CWA for Windows** :

      i. Validate that group policy on the client (add more detail and SS for this) is appropriately set and does not conflict with the rules set in Studio.

      ii. Validate that default rules in the client's registry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`

b. CWA for Linux - To triage CWA for Linux issues, see USB documentation for CWA for Linux

c. CWA for Mac - To triage CWA for Mac issues, see CWA for Mac

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- On TSVDA, audio devices are blocked by default from using USB redirection. The recommended way to use those devices is using the optimized Audio VC.
- Sometimes, USB composite devices might not be split automatically even though a correct device redirection rule is set to split the device. This issue occurs because the device is in low power mode. In these instances, the child device that enters low power mode might not be present in the device list. You can use the following workarounds to overcome this issue:
  - Disconnect the session, insert the USB device, and reconnect to the session.
  - Unplug the USB device and plug it back in. This action results in the device moving out of low power mode.
- Sometimes, USB battery saver settings may be enabled to optimize battery life. If the client endpoint goes to sleep, the USB device may get disconnected. In such a scenario, you might have to disconnect and reconnect the device in order to present the device again in the session.

Event Logs

Administrators can now monitor for unauthorized devices that users may attempt to redirect and can take the appropriate action. Here are some of the event messages that will be logged in the Event viewer on the VDA host for devices that are allowed to be redirected and for devices that are not.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB Diagnostics Tool

`CtxUsbDiagnostics.exe` is a command-line tool on the VDA to help Citrix admins diagnose and resolve USB device redirection issues experienced on the client in an expedited manner. This utility tool collects vital information required to triage configuration issues associated with USB devices attached to the client that are failing to redirect inside an HDX session.

```
> **Note :**

>

> Running Command Prompt or Powershell as an administrator is required to ensure the tool has the necessary permissions to perform system-level operations.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements

Session host

- Operating system
  - Windows 10 1809 or later
  - Windows 11 21H2 or later
  - Windows Server 2016 or later
- VDA
  - Windows: Citrix Virtual Apps and Desktops™ Version 2311 or later

Client device

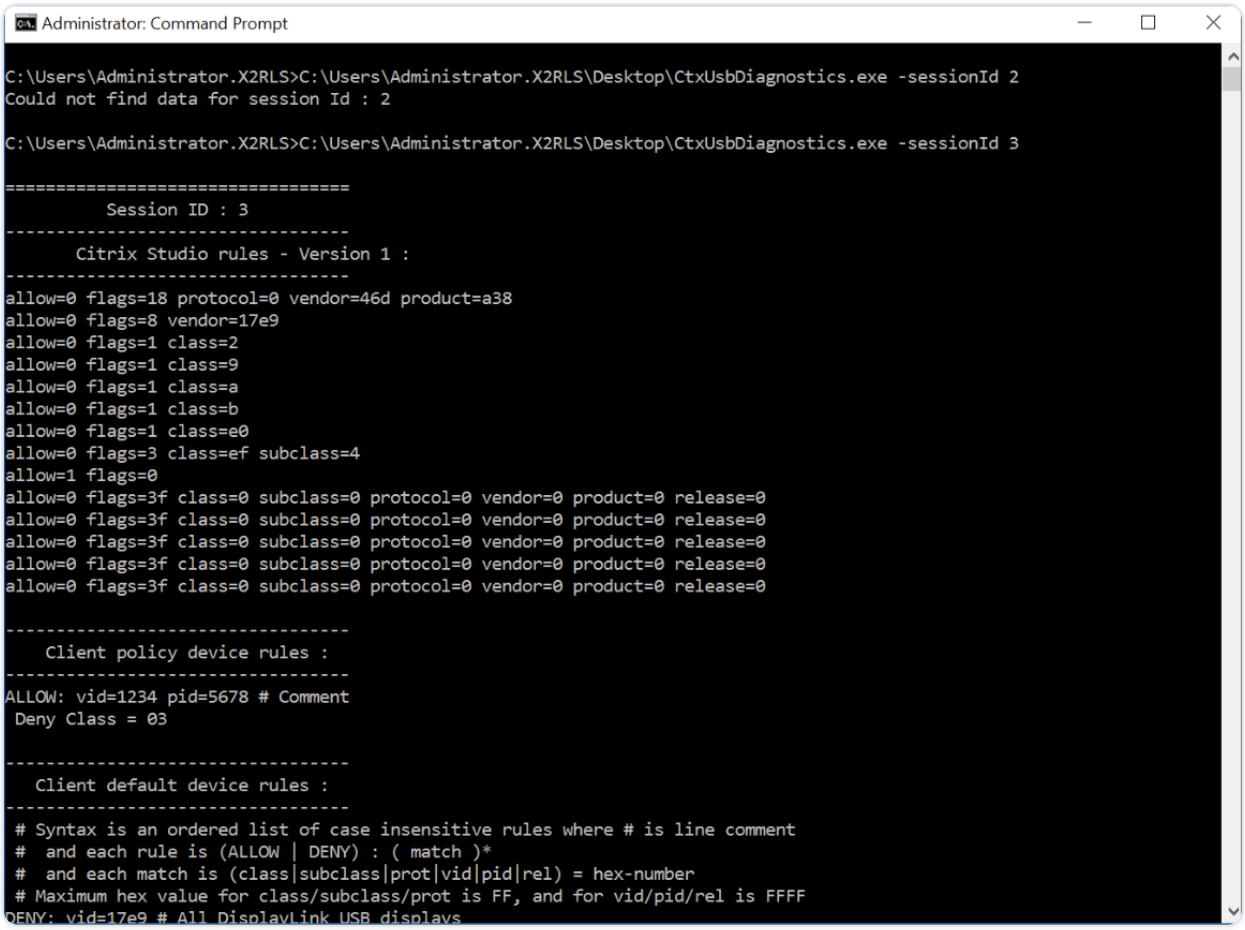
- Operating system
  - Windows 10 1809 or later
- Workspace App
  - Windows: version 2311 or later

What does the tool do?

The tool currently provides:

- SessionID
- VDA device policies (device rules set in Studio)
- Client devices and client device policies (device rules)
- List of devices, their redirection state, and why they were allowed or denied

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE :

The administrator can see device information for all active sessions.

Information Displayed

- **Citrix Studio rules - Version 1/2**
  - The DDC rules indicate the use of the legacy “**Client USB device redirection rules**” or “**Client USB device redirection rules (Version 2)**” policy in Studio. The information listed in this section lists all the rules configured by the Citrix® admin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

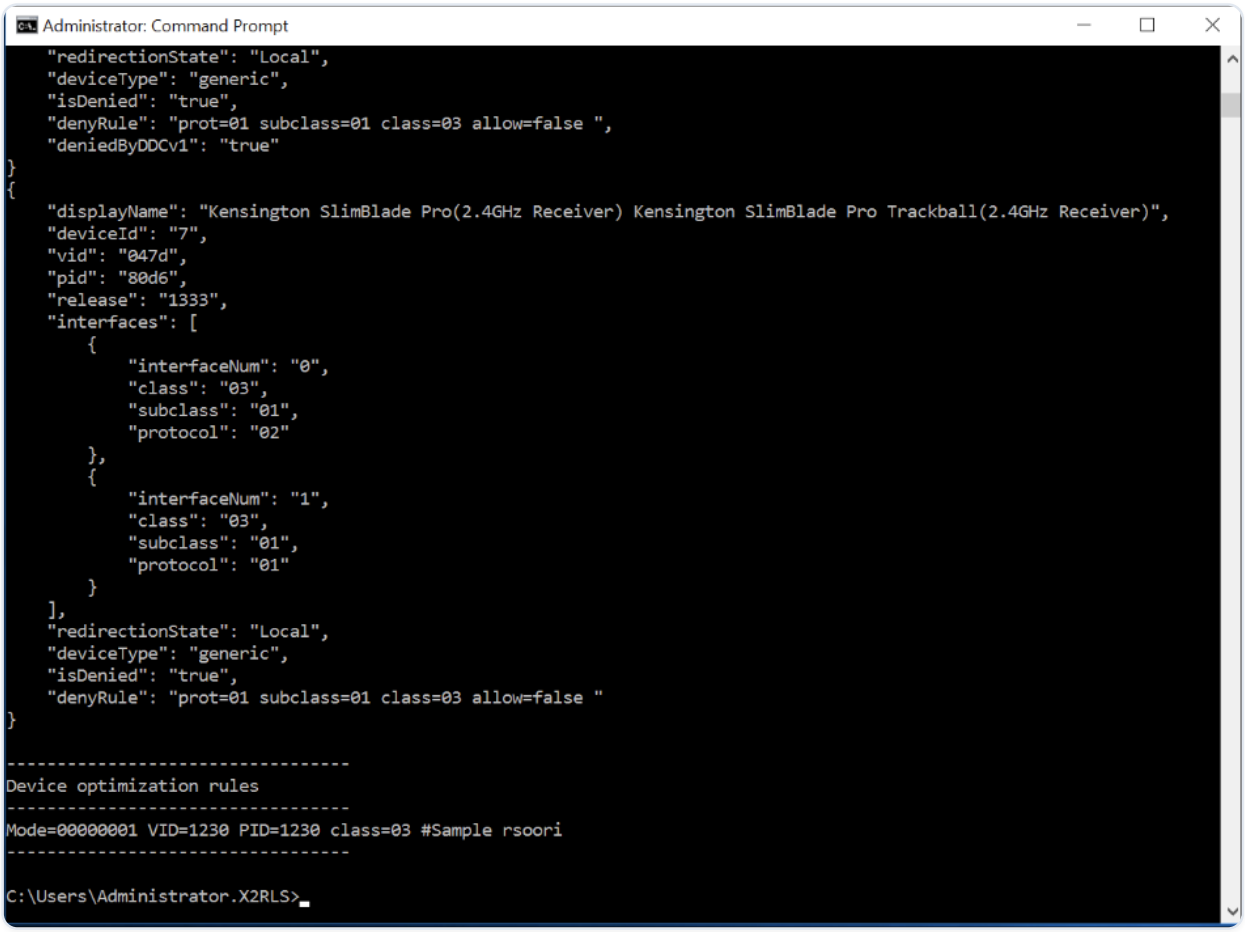
---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **Client Default Device Rules**
  - This section lists the rules that are set in the registry on the client.

```
---------------------------------
  Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **Device optimization rules**
  - The section lists the device optimization rules as set in "Client USB device optimization rules.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Device List

This section lists valuable information about each device that is connected to the client endpoint, the hardware information, whether it is being redirected or not, whether the correct device redirection rule is set or not, and so on.

TAG NAME	DESCRIPTION
displayName	Lists the common name of the device.
vid	Vendor ID
pid	Product ID
Interfaces	This subsection lists all the interfaces in case the composite device has been split into multiple child devices.
InterfaceNum	Indicates the index of the interface descriptor
class	Class code

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TAG NAME	DESCRIPTION
subclass	Subclass Code
protocol	Protocol
redirectionState	**Local** indicates that the device is not redirected in the ICA® session. **ThisSession** indicates that the device is redirected in the ICA session. **OtherSession** indicates that the device is redirected in another ICA session.
optiEnabled	**true** indicates that the device is optimized. **false** indicates that the device is not optimized and the data transfer happens over the USB virtual channel.
deviceType	**generic** indicates that the device does not have an optimized virtual channel and the traffic is flowing through the USB virtual channel. **optimized** implies that the data transfer associated with the device is happening over a dedicated virtual channel.
isDenied	**true** indicates that the device is not redirected because of a policy rule set by the admin. `false` indicates that the device is redirected because of applied policy.
denyRule	This field is useful if **isDenied** is set to `true`. It tells the admin the specific rule set in the policy that is resulting in the device not getting redirected.

Legacy USB Redirection Configuration

If you are using any components older than version 2212 or if you are using CWA for Linux, follow this guide for configuring USB redirection in your environment.

Enabling Generic USB Redirection

1. Open **Citrix Web Studio™ policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA® > USB Devices policies**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Edit the **Client USB device redirection policy**.
4. Select **Allowed** and click **Save**.

Creating USB Redirection Policy Rules

When the user tries to redirect a USB device to Virtual Desktop, it is checked against each USB policy rule in turn until a match is found. The first match for any devices is considered final. If the first match is an Allow rule, the matched device is allowed to be redirected to the virtual desktop. If the first match is a Deny rule, the matched device is only available in the local desktop. If no match is found, default rules are used.

Setting the policy on the DDC:

1. Open **Citrix Web Studio policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA > USB Devices policies**.
3. Edit the **Client USB device redirection rules**.
4. Set the value based on the examples provided in the description for each usb device that needs to be redirected and click Save. For Example: Allow: VID=056A PID=00A4 #STU-430 Deny: Class=08 subclass=05 # Mass Storage

   NOTE:

   If a Citrix® admin checks Use default value and clicks on Save, the default rules can be found in the following registry in the VDA.

   Caution!:
   Refer to the Disclaimer at the end of this article before using the Registry Editor.
   `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

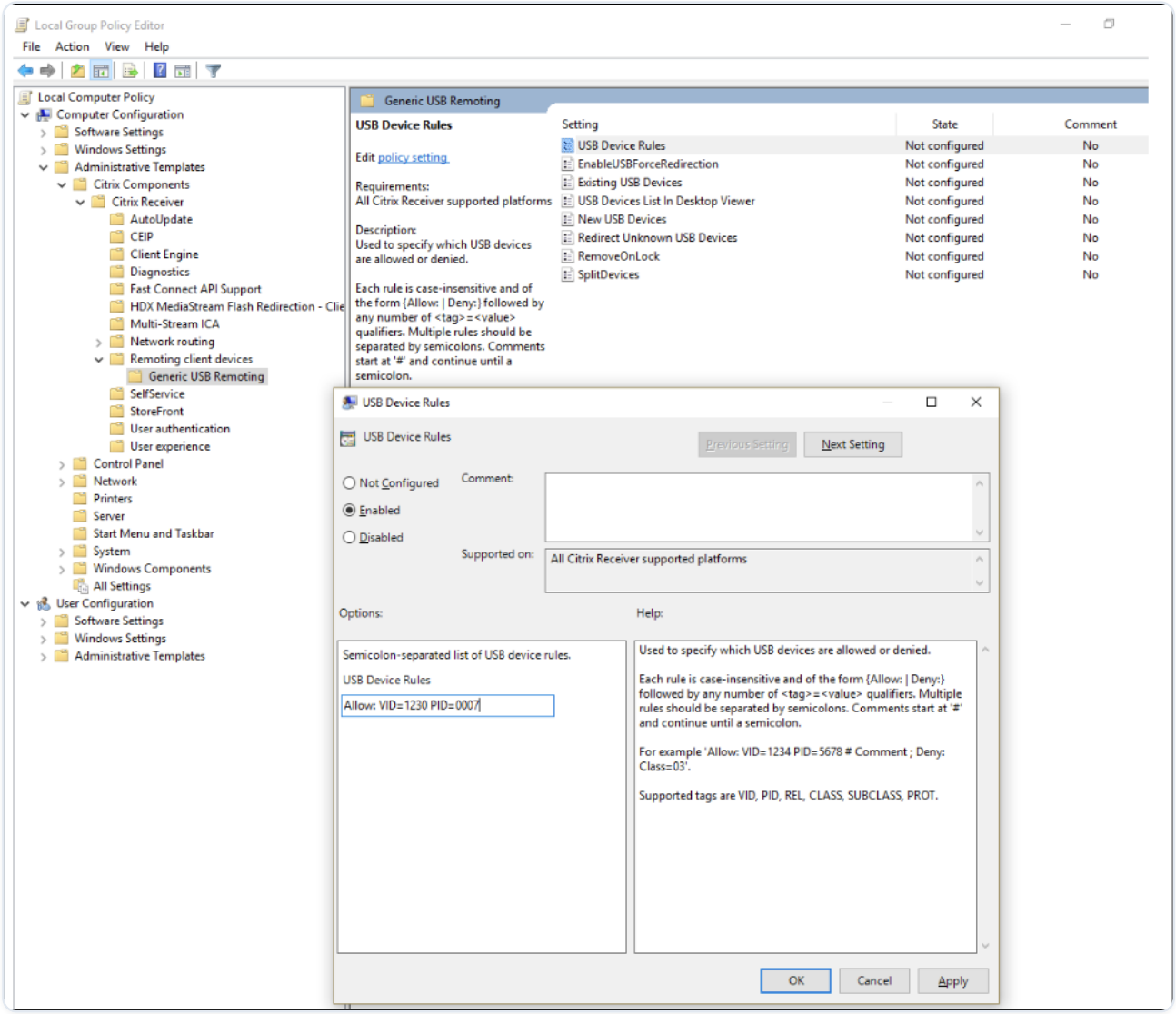
Using GPOs on the client:

1. Open the **Local Group Policy Editor** and go to **Administrative Templates > Citrix Components > Citrix Receiver™ > Remoting client devices > Generic USB Remoting**.
2. Open the **USB Device Rules setting** and enable the setting. Add the USB Device rule as in this example, The Allow: VID=1230 PID=0007 rule allows the device with Vendor ID 1230 and Product ID 0007.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Use the Allow: VID=xxxx PID=xxxx rule when a specific device must be on top of the device rules list.



NOTE:

A tool like USBView or even the Connection toolbar can be used to determine the device details like VID and PID (include SS here).

Configure automatic redirection of USB devices

USB devices are automatically redirected when USB support is enabled. Also, the USB user preference settings are set to automatically connect USB devices. It is not always best to redirect all USB devices. Users can explicitly redirect devices from the USB device list that are not

© 1997–2026 Citrix Systems, Inc. All rights reserved.

automatically redirected. To prevent USB devices from being listed or redirected, use DeviceRules on either the client endpoint or the DDC policy.

This policy can be set either on the DDC, on the client using a GPO, using Citrix Workspace™ app Preferences or the Connections tab under CDViewer. All of these methods are described below:

Setting the policy on the DDC:

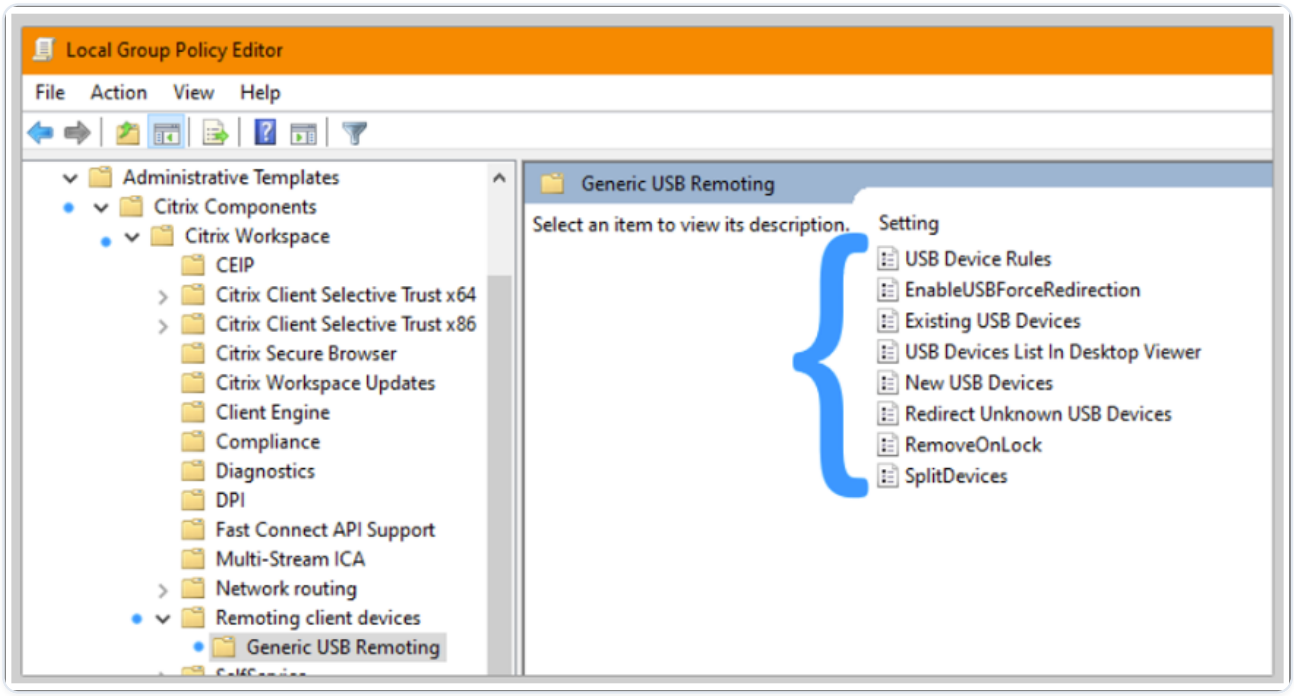
There are two policies on the DDC that can be set to allow auto redirection of USB devices- “Allow existing USB devices to be automatically connected, Allow newly arrived USB devices to be automatically connected’

1. Open **Citrix Web Studio policies** and click on the **Policies** tab.
2. Click on **Create Policy** and expand the **ICA > USB Devices policies**.
3. Edit the setting **Allow existing USB devices to be automatically connected**.
4. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.
5. Edit the setting **Allow newly arrived USB devices to be automatically connected**.
6. Clear the **Use default value** checkbox and select **Automatically redirect available USB devices** from the drop down menu and click **Save**.

Using GPOs on the client:

1. Open **Local Group Policy Editor** and go to **Administrative Templates > Citrix Components > Citrix Receiver > Remoting client devices > Generic USB Remoting**.
2. Open **New USB Devices**, select **Enabled**, and click **OK**.
3. Open **Existing USB Devices**, select **Enabled**, and click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



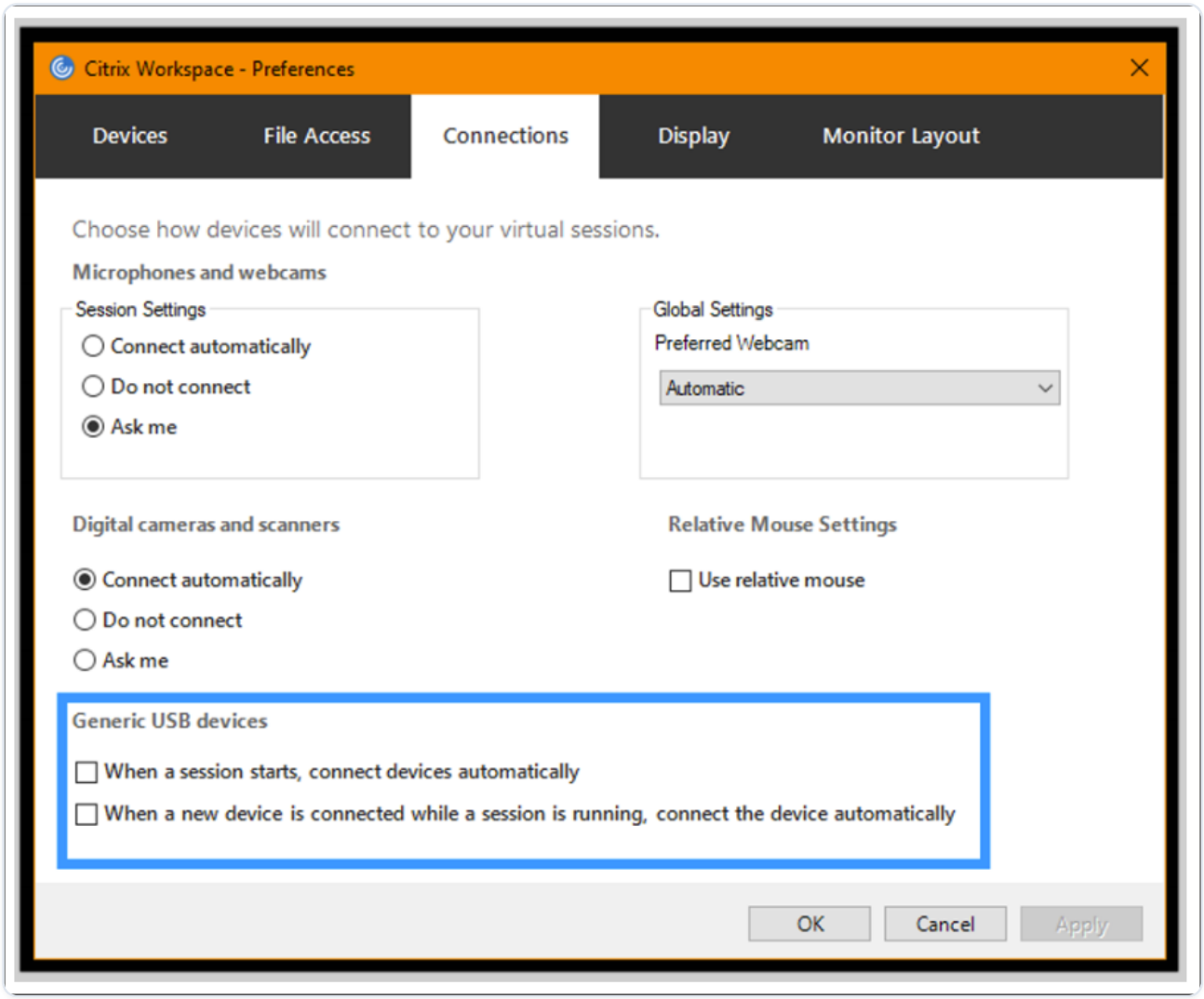
Using Citrix Connection Center:

1. Go to **Citrix Workspace Preferences > Connections**.
2. Ensure that the following options are selected:
    a. When a session starts, connect devices automatically
    b. When a new device is connected while a session is running, connect the device automatically.
3. Click **OK**.

Using CDViewer Connection toolbar:

1. After a session starts, click on the **CDViewer** dropdown and select the **Citrix Workspace Preferences > Connections** tab.
2. Ensure that the following options are selected:
    a. When a session starts, connect devices automatically
    b. When a new device is connected while a session is running, connect the device automatically.
3. Click **Apply** and **OK** to save the policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For the client based configurations, the registry keys are set to the client device at the following location:

CAUTION!:

Refer to the Disclaimer at the end of this article before using the Registry Editor.

`HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Graphics

Citrix HDX graphics include an extensive set of graphics acceleration and encoding technologies that optimizes the delivery of rich graphics applications from Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service). The graphic technologies provide the same experience as using a physical desktop when working remotely with virtual applications that are graphics intensive.

You can use software or hardware for graphics rendering. Software rendering requires a third-party library called software rasterizer. For example, Windows includes the WARP rasterizer for DirectX based graphics. Sometimes, you might want to use an alternative software renderer. Hardware rendering (hardware acceleration) requires a graphics processor (GPU).

HDX™ Graphics offers a default encoding configuration that is optimized for the most common use cases. By using Citrix policies, IT administrators can also configure various graphics-related settings to meet different requirements and provide the desired user experience.

Thinwire

Thinwire is the Citrix default display remoting technology used in Citrix DaaS.

Display remoting technology allows graphics generated on one machine to be transmitted, typically across a network, to another machine for display. Graphics are generated as a result of user input, for example, keystrokes or mouse actions.

HDX 3D Pro

The HDX 3D Pro capabilities in Citrix DaaS enable you to deliver desktops and applications that perform best using a graphics processing unit (GPU) for hardware acceleration. These applications include 3D professional graphics applications based on OpenGL and DirectX. The standard VDA supports GPU acceleration of DirectX only.

GPU acceleration for Windows Single-session OS

By using HDX 3D Pro, you can deliver graphically intensive applications as part of hosted desktops or applications on Single-session OS machines. HDX 3D Pro supports physical host computers (including desktop, blade, and rack workstations) and GPU Passthrough and GPU virtualization technologies offered by XenServer®, vSphere, and Hyper-V (passthrough only) hypervisors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using GPU Passthrough, you can create VMs that have exclusive access to dedicated graphics processing hardware. You can install multiple GPUs on the hypervisor and assign VMs to each of these GPUs on a one-to-one basis.

Using GPU virtualization, multiple virtual machines can directly access the graphics processing power of a single physical GPU.

GPU acceleration for Windows Multi-session OS

HDX 3D Pro allows graphics-heavy applications running in Windows Multi-session OS sessions to render on the server graphics processing unit (GPU). By moving OpenGL, DirectX, Direct3D, and Windows Presentation Foundation (WPF) rendering to the server GPU, graphics rendering doesn't slow down the server CPU. Also, the server is able to process more graphics because the workload is split among the CPU and GPU.

Framehawk

IMPORTANT:

As of Citrix Virtual Apps and Desktops 7 1903, Framehawk is no longer supported. Instead, use Thinwire with adaptive transport enabled.

Framehawk is a display remoting technology for mobile workers on broadband wireless connections (Wi-Fi and 4G/LTE cellular networks). Framehawk overcomes the challenges of spectral interference and multipath propagation and delivers a fluid and interactive user experience to users of virtual apps and desktops.

Text-based session watermark

Text-based session watermarks help to deter and enable tracking data theft. This traceable information appears on the session desktop as a deterrent to those using photographs and screen captures to steal data. You can specify a watermark that is a layer of text. The watermark can display over the entire session screen without changing the content of the original document. Text-based session watermarks require VDA support.

Related information

- HDX 3D Pro
- GPU acceleration for Windows Single-session OS
- GPU acceleration for Windows Multi-session OS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Thinwire
- Text-based session watermark

HDX™ 3D Pro

The HDX 3D Pro capabilities of Citrix Virtual Apps and Desktops™ enable you to deliver desktops and applications that perform best using a graphics processing unit (GPU) for hardware acceleration. These applications include 3D professional graphics applications based on OpenGL and DirectX. The standard VDA supports GPU acceleration of DirectX only.

For the HDX 3D Pro policy settings, see Optimize for 3D graphics workload.

All supported Citrix Workspace apps can be used with 3D graphics. For best performance with complex 3D workloads, high-resolution monitors, multi-monitor configurations, and high frame rate applications, we recommend the latest versions of Citrix Workspace app for Windows and Citrix Workspace app for Linux. For more information on supported versions of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app.

Examples of 3D professional applications include:

- Computer-aided design, manufacturing, and engineering (CAD/CAM/CAE) applications
- Geographical Information System (GIS) software
- Picture Archiving Communication System (PACS) for medical imaging
- Applications using the latest OpenGL, DirectX, NVIDIA CUDA, and OpenCL and WebGL versions
- Computationally intensive non-graphical applications that use NVIDIA Compute Unified Device Architecture (CUDA) GPUs for parallel computing

HDX 3D Pro provides the best user experience over any bandwidth:

- On WAN connections: Deliver an interactive user experience over WAN connections with bandwidths as low as 1.5 Mbps.
- On LAN connections: Deliver a user experience equivalent to that of a local desktop on LAN connections.

  You can replace complex and expensive workstations with simpler user devices by moving the graphics processing into the data center for centralized management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX 3D Pro provides GPU acceleration for Windows single-session OS machines and Windows multi-session OS machines. For more information, see GPU acceleration for Windows single-session OS and GPU acceleration for Windows multi-session OS.

HDX 3D Pro is compatible with GPU passthrough and GPU virtualization technologies offered by the following hypervisors, in addition to bare metal:

- XenServer®
  - GPU passthrough with NVIDIA GRID, AMD, and Intel GVT-d
  - GPU virtualization with NVIDIA GRID, AMD, and Intel GVT-g
  - See hardware compatibility at Hypervisor Hardware Compatibility List.

Use the HDX Monitor tool to validate the operation and configuration of HDX visualization technologies and to diagnose and troubleshoot HDX issues. To download the tool and learn more about it, see `<https://taas.citrix.com/hdx/download/>`.

GPU acceleration for Windows multi-session OS

HDX™ 3D Pro allows graphics-heavy applications running in Windows Multi-session OS sessions to render on the server's graphics processing unit (GPU). By moving OpenGL, DirectX, Direct3D, and Windows Presentation Foundation (WPF) rendering to the server's GPU, graphics rendering does not slow the server's CPU. Also, the server is able to process more graphics because the workload is split between the CPU and GPU.

Since Windows Server is a multi-user operating system, multiple users can share a GPU accessed by Citrix Virtual Apps™ without the need for GPU virtualization (vGPU).

For procedures that involve editing the registry, use caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

GPU sharing

GPU Sharing enables GPU hardware rendering of OpenGL and DirectX applications in remote desktop sessions. It has the following characteristics:

- Can be used on bare metal or virtual machines to increase application scalability and performance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Enables multiple concurrent sessions to share GPU resources (most users do not require the rendering performance of a dedicated GPU).
- Requires no special settings.

A GPU can be assigned to the Windows Server virtual machine in either full pass-through or virtual GPU (vGPU) modes following Hypervisor and GPU vendor requirements. Bare-metal deployments on physical Windows Server machines are also supported.

GPU Sharing does not depend on any specific graphics card.

- For virtual machines, select a graphics card that is compatible with the Hypervisor in use. For a XenServer hardware compatibility list, see Hypervisor Hardware Compatibility List.
- When running on bare metal, it is recommended to have a single display adapter enabled by the operating system. If multiple GPUs are installed on the hardware, disable all but one of them using Device Manager.

Scalability using GPU Sharing depends on several factors:

- The applications being run
- The amount of video RAM they consume
- The graphics card's processing power

Some applications handle video RAM shortages better than others. If the hardware becomes overloaded, instability or a crash of the graphics card driver might occur. Limit the number of concurrent users to avoid such issues.

To confirm that GPU acceleration is occurring, use a third-party tool such as GPU-Z. GPU-Z is available at `<http://www.techpowerup.com/gpuz/>`.

- Access to a high-performance video encoder for NVIDIA GPUs and Intel Iris Pro graphics processors. A policy setting (enabled by default) controls this feature and allows the use of hardware encoding for H.264 encoding (where available). If such hardware is not available, the VDA fall backs to CPU-based encoding using the software video codec. For more information, see Graphics policy settings.

DirectX, Direct3D, and WPF rendering

DirectX, Direct3D, and WPF rendering are only available on servers with a GPU that supports a display driver interface (DDI) version of 9ex, 10, or 11.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On Windows Server 2008 R2, DirectX and Direct3D require no special settings to use a single GPU.
- On Windows Server 2012 and later, Remote Desktop Services (RDS) sessions on the RD Session Host server use the Microsoft Basic Render Driver as the default adapter. To use the GPU in RDS sessions on Windows Server 2012 and later, enable the **Use the hardware default graphics adapter for all Remote Desktop Services sessions** setting in the group policy **Local Computer Policy** \> **Computer Configuration** \> **Administrative Templates** \> **Windows Components** \> **Remote Desktop Services** \> **Remote Desktop Session Host** \> **Remote Session Environment**.
- To enable WPF applications to render using the server's GPU, create the settings in the registry of the server running Windows Multi-session OS sessions. For information on the registry setting, see Windows Presentation Foundation (WPF) rendering in the list of features managed through the registry.

GPU acceleration for CUDA or OpenCL applications

GPU acceleration of CUDA and OpenCL applications running in a user session is disabled by default.

To use the CUDA acceleration POC features, enable the registry settings. For information, see GPU acceleration for CUDA or OpenCL applications in the list of features managed through the registry.

GPU acceleration for Windows single-session OS

With HDX 3D Pro, you can deliver graphically intensive applications as part of hosted desktops or applications on Single-session OS machines. HDX 3D Pro supports physical host computers (including desktop, blade, and rack workstations) and GPU Passthrough and GPU virtualization technologies offered by XenServer®, vSphere, Nutanix, and Hyper-V (passthrough only) hypervisors.

HDX™ 3D Pro offers the following features:

- Adaptive H.264-based or H.265-based deep compression for optimal WAN and wireless performance. HDX 3D Pro uses CPU-based full-screen H.264 compression as the default compression technique for encoding. Hardware encoding with H.264 is used with NVIDIA, Intel, and AMD cards that support NVENC. Hardware encoding with H.265 is used with NVIDIA cards that support NVENC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Lossless compression option for specialized use cases. HDX 3D Pro also offers a CPU-based lossless codec to support applications where pixel-perfect graphics are required, such as medical imaging. True lossless compression is recommended only for specialized use cases because it consumes more network and processing resources.

  When using lossless compression:

  - The lossless indicator, a notification area icon, notifies the user if the screen displayed is a lossy frame or a lossless frame. This icon helps when the **Visual Quality** policy setting specifies **Build to lossless**. The lossless indicator turns green when the frames sent are lossless.
  - The lossless switch enables the user to change to Always Lossless mode anytime within the session. To select or deselect **Lossless anytime within a session**, right-click the icon and click **Switch to pixel perfect** or use the shortcut ALT+SHIFT+1.

    For lossless compression: HDX 3D Pro uses the lossless codec for compression regardless of the codec selected through policy.

    For lossy compression: HDX 3D Pro uses the original codec, either the default or the one selected through policy.

    Lossless switch settings are not retained for subsequent sessions. To use a lossless codec for every connection, select **Always lossless** in the **Visual quality** policy setting.

- You can override the default shortcut, ALT+SHIFT+1, to select or deselect Lossless within a session. Configure a new registry setting at `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`.

  - Name: HKLM_Hotkey, Type: String
  - The format to configure a shortcut combination is C=0`|`1, A=0`|`1, S=0`|`1, W=0`|`1, K=val. Keys must be comma "," separated. The order of the keys does not matter.
  - A, C, S, W and K are keys, where C=Control, A=ALT, S=SHIFT, W=Win, and K=a valid key. Allowed values for K are 0–9, a–z, and any virtual key code.
  - For example:
    - For F10, set K=0x79
    - For Ctrl + F10, set C=1, K=0x79
    - For Alt + A, set A=1, K=a or A=1, K=A or K=A, A=1
    - For Ctrl + Alt + 5, set C=1, A=1, K=5 or A=1, K=5, C=1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For Ctrl + Shift + F5, set A=1, S=1, K=0x74

CAUTION:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

- Multiple and high resolution monitor support. For Single-session OS machines, HDX 3D Pro supports user devices with up to four monitors. Users can arrange their monitors in any configuration and can mix monitors with different resolutions and orientations. The number of monitors is limited by the capabilities of the host computer GPU, the user device, and the available bandwidth. HDX 3D Pro supports all monitor resolutions and is limited only by the capabilities of the GPU on the host computer.
- Dynamic resolution. You can resize the virtual desktop or application window to any resolution. **Note**: The only supported method to change the resolution is by resizing the VDA session window. Changing resolution from within the VDA session (using **Control Panel > Appearance** and **Personalization > Display > Screen Resolution) is not supported**.
- Support for NVIDIA vGPU architecture. HDX 3D Pro supports NVIDIA vGPU cards. For information, see NVIDIA vGPU for GPU passthrough and GPU sharing. NVIDIA vGPU enables multiple VMs to have simultaneous, direct access to a single physical GPU, using the same NVIDIA graphics drivers that are deployed on non-virtualized operating systems.
- Support for VMware vSphere and VMware ESX using Virtual Direct Graphics Acceleration (vDGA) - You can use HDX 3D Pro with vDGA for both RDS and VDI workloads.
- Support for VMware vSphere/ESX using NVIDIA vGPU and AMD MxGPU.
- Support for Microsoft HyperV using Discrete Device Assignment in Windows Server 2016.
- Support for Data Center Graphics with Intel Xeon Processor E3 Family. HDX 3D Pro supports multi-monitors (up to 3), console blanking, custom resolution, and high frame-rate with the supported family of Intel processors. For more information, see `<http://www.citrix.com/intel>`.
- Support for AMD RapidFire on the AMD FirePro S-series server cards. HDX 3D Pro supports multi-monitors (up to 6), console blanking, custom resolution, and high frame-rate. Note: HDX 3D Pro support for AMD MxGPU (GPU virtualization) works with VMware vSphere vGPUs only. XenServer and Hyper-V are supported with GPU passthrough. For more information, see AMD Virtualization Solution.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

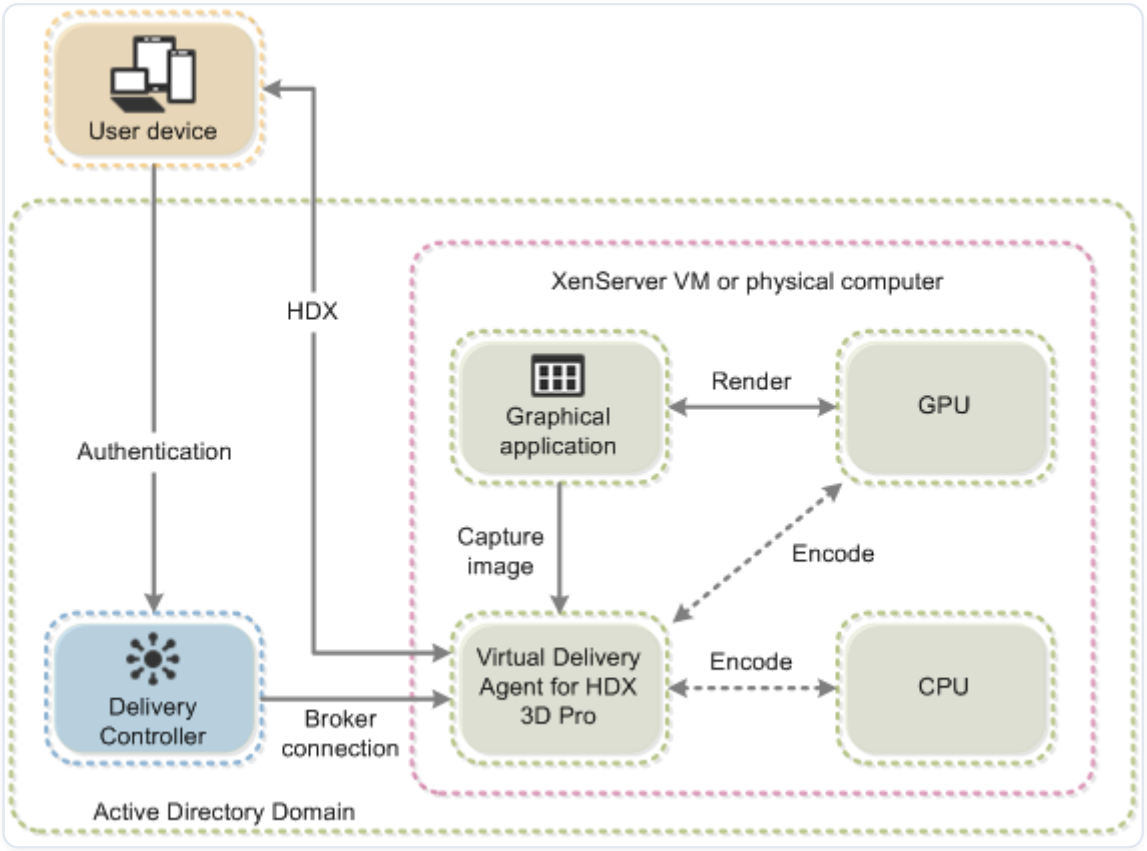
- Access to a high-performance video encoder for NVIDIA GPUs, AMD GPUs, and Intel Iris Pro graphics processors. A policy setting (enabled by default) controls this feature. The feature allows the use of hardware encoding for H.264 encoding (where available). If such hardware is not available, the VDA falls back to CPU-based encoding using the software video codec. For more information, see Graphics policy settings.

As shown in the following figure:

- When a user logs on to Citrix Workspace™ app and accesses the virtual application or desktop, the Controller authenticates the user. The Controller then contacts the VDA for HDX 3D Pro to broker a connection to the computer hosting the graphical application.

The VDA for HDX 3D Pro uses the appropriate hardware on the host to compress views of the complete desktop or of just the graphical application.

- The desktop or application views and the user interactions with them are transmitted between the host computer and the user device. This transmission is done through a direct HDX connection between Citrix Workspace app and the VDA for HDX 3D Pro.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Optimize the HDX 3D Pro user experience

To use HDX 3D Pro with multiple monitors, ensure that the host computer is configured with at least as many monitors as are attached to user devices. The monitors attached to the host computer can be either physical or virtual.

Do not attach a monitor (either physical or virtual) to a host computer while a user is connected to the virtual desktop or application providing the graphical application. Doing so can cause instability during a user's session.

Let your users know that changes to the desktop resolution (by them or an application) are not supported while a graphical application session is running. After closing the application session, a user can change the resolution of the Desktop Viewer window in the Citrix Workspace app - Desktop Viewer Preferences.

When multiple users share a connection with limited bandwidth (for example, at a branch office), we recommend that you use the **Overall session bandwidth limit** policy setting to limit the bandwidth available to each user. Using this setting ensures that the available bandwidth does not fluctuate widely as users log on and off. Because HDX 3D Pro automatically adjusts to use all the available bandwidth, large variations in the available bandwidth over the course of user sessions can negatively impact performance.

For example, if 20 users share a 60 Mbps connection, the bandwidth available to each user can vary between 3 Mbps and 60 Mbps, depending on the number of concurrent users. To optimize the user experience in this scenario, determine the bandwidth required per user at peak periods and limit users to this amount always.

For users of a 3D mouse, we recommend that you increase the priority of the Generic USB Redirection virtual channel to 0. For information about changing the virtual channel priority, see the Knowledge Center article CTX128190.

Thinwire

Introduction

Thinwire, a part of Citrix HDX technology, is the Citrix default display remoting technology used in Citrix Virtual Apps and Desktops.

Display remoting technology allows graphics generated on one machine to be transmitted, typically across a network, to another machine for display.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A successful display remoting solution provides a highly interactive user experience that is similar to that of a local PC. Thinwire achieves this experience by using a range of complex and efficient image analysis and compression techniques. Thinwire maximizes server scalability and consumes less bandwidth than other display remoting technologies.

Because of this balance, Thinwire meets most general business use cases and is used as the default display remoting technology in Citrix Virtual Apps and Desktops.

HDX™ 3D Pro

In its default configuration, Thinwire can deliver 3D or highly interactive graphics and use a graphics processing unit (GPU), if present. However, we recommend enabling HDX 3D Pro mode using the **Optimize for 3D graphics workload** or **Visual quality > Build to lossless** policies for scenarios when GPUs are present. These policies configure Thinwire to use a video codec (H.264 or H.265) to encode the entire screen using hardware acceleration if a GPU is present. Doing so provides a more fluid experience for 3D professional graphics. For more information, see H.264 Build to lossless, HDX 3D Pro, and GPU acceleration for Windows Single-session OS.

Requirements

Thinwire is optimized for modern operating systems, including Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, and Windows 10. For Windows Server 2008 R2, legacy graphics mode is recommended. Use the built-in Citrix policy templates, High Server Scalability-Legacy OS and Optimized for WAN-Legacy OS to deliver the Citrix recommended combinations of policy settings for these use cases.

NOTE:

We do not support legacy graphics mode in this release. It is included for backward compatibility when using XenApp 7.15 LTSR, XenDesktop 7.15 LTSR, and previous VDA releases.

- The policy setting which drives the behavior of Thinwire, **Use video codec for compression**, is available on VDA versions in Citrix Virtual Apps and Desktops 7 1808 or later and XenApp and XenDesktop 7.6 FP3 and later. The **Use video codec when preferred** option is the default setting on VDA versions Citrix Virtual Apps and Desktops 7 1808 or later and XenApp and XenDesktop 7.9 and later.
- All Citrix Workspace™ apps support Thinwire. Some Citrix Workspace apps might support features of Thinwire that others do not, for example, 8-bit or 16-bit graphics for reduced

© 1997–2026 Citrix Systems, Inc. All rights reserved.

bandwidth usage. Support for such features is automatically negotiated by Citrix Workspace app.

- Thinwire uses more server resources (CPU, memory) in multi-monitor and high-resolution scenarios. It is possible to tune the amount of resources Thinwire uses, however, bandwidth usage might increase as a result.
- In low bandwidth or high latency scenarios, consider enabling 8-bit or 16-bit graphics to improve interactivity. Visual quality might be affected, especially at 8-bit color depth.

Encoding methods

Thinwire can operate in two different encoding modes depending on policy and client capabilities:

- Thinwire full screen H.264 or H.265
- Thinwire with selective H.264 or H.265

Legacy GDI remoting uses the XPDM remoting driver and not a Thinwire bitmap encoder.

Configuration

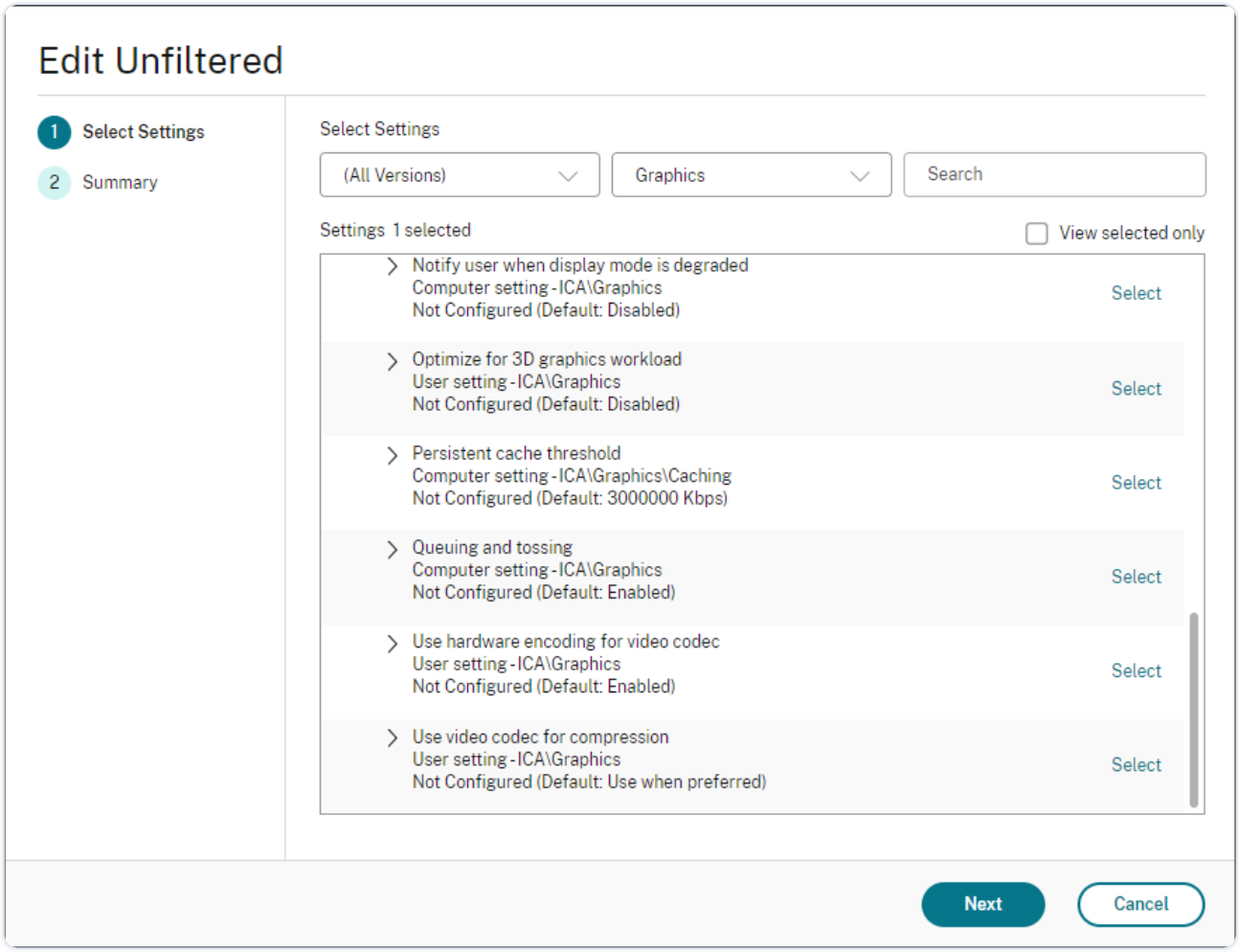
Thinwire is the default display remoting technology.

The following Graphics policy setting sets the default and provides alternatives for different use cases:

- Use video codec for compression
  - **Use video codec when preferred**. This is the default setting. No additional configuration is required. Keeping this setting as the default ensures that Thinwire is selected for all Citrix connections, and is optimized for scalability, bandwidth, and superior image quality for typical desktop workloads. This is functionally equivalent to **For actively changing regions**.
- Other options in this policy setting continue to use Thinwire with other technologies for different use cases. For example:
  - **For actively changing regions**. The adaptive display technology in Thinwire identifies moving images (video, 3D in motion) and uses H.264 or H.265 only in the part of the screen where the image is moving.
  - **For the entire screen**. Delivers Thinwire with full-screen H.264 or H.265 to optimize for improved user experience and bandwidth in cases with heavy use of 3D graphics. In the case of H.264 4:2:0 (the **Visually lossless** policy is disabled), the final image is not pixel

© 1997–2026 Citrix Systems, Inc. All rights reserved.

perfect (lossless) and might not be suitable for certain scenarios. In such cases, consider using H.264 Build to lossless instead.



Various other policy settings, including the following Visual display policy settings can be used to fine tune the performance of display remoting technology. Thinwire supports them all.

- Preferred color depth for simple graphics
- Target frame rate
- Visual quality

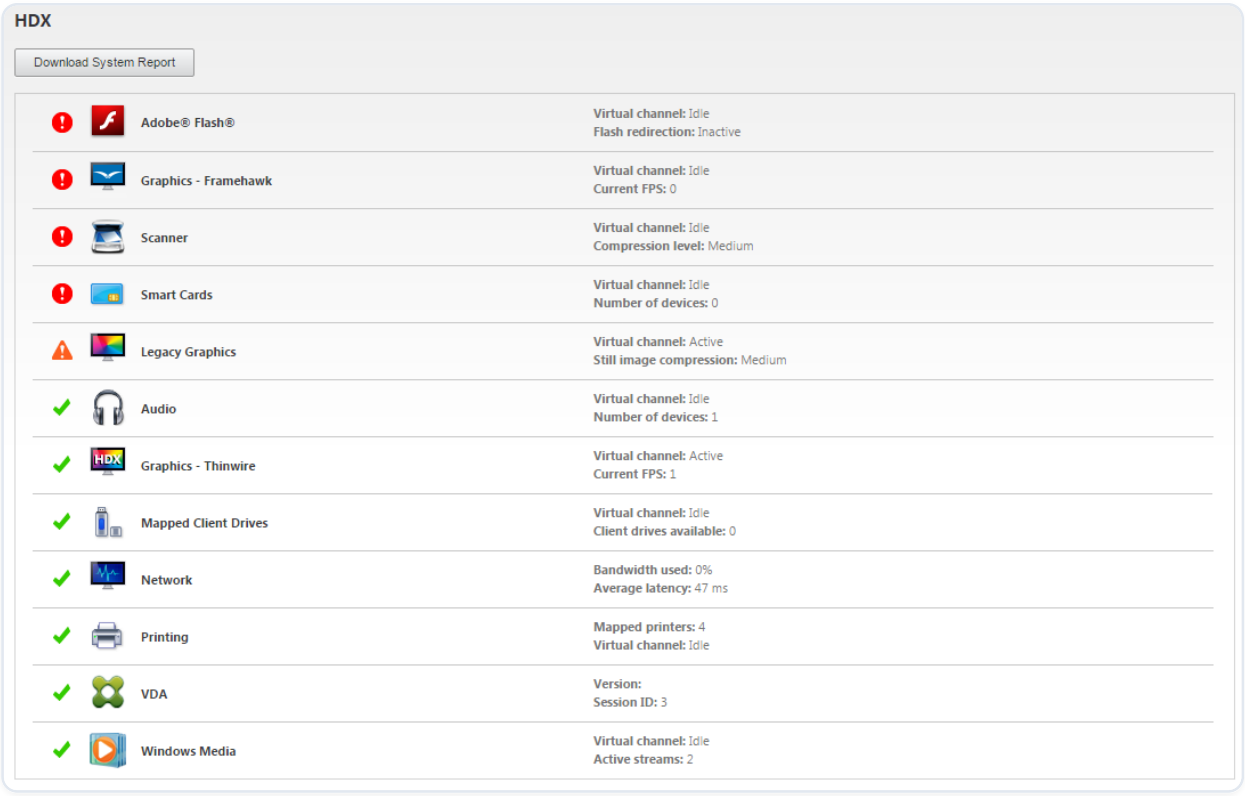
To get the Citrix recommended combinations of policy settings for different business use cases, use the built-in Citrix Policy templates. The **High Server Scalability** and **Very High Definition User Experience** templates both use Thinwire with the optimum combinations of policy settings for your organization's priorities and your users' expectations.

Monitoring Thinwire

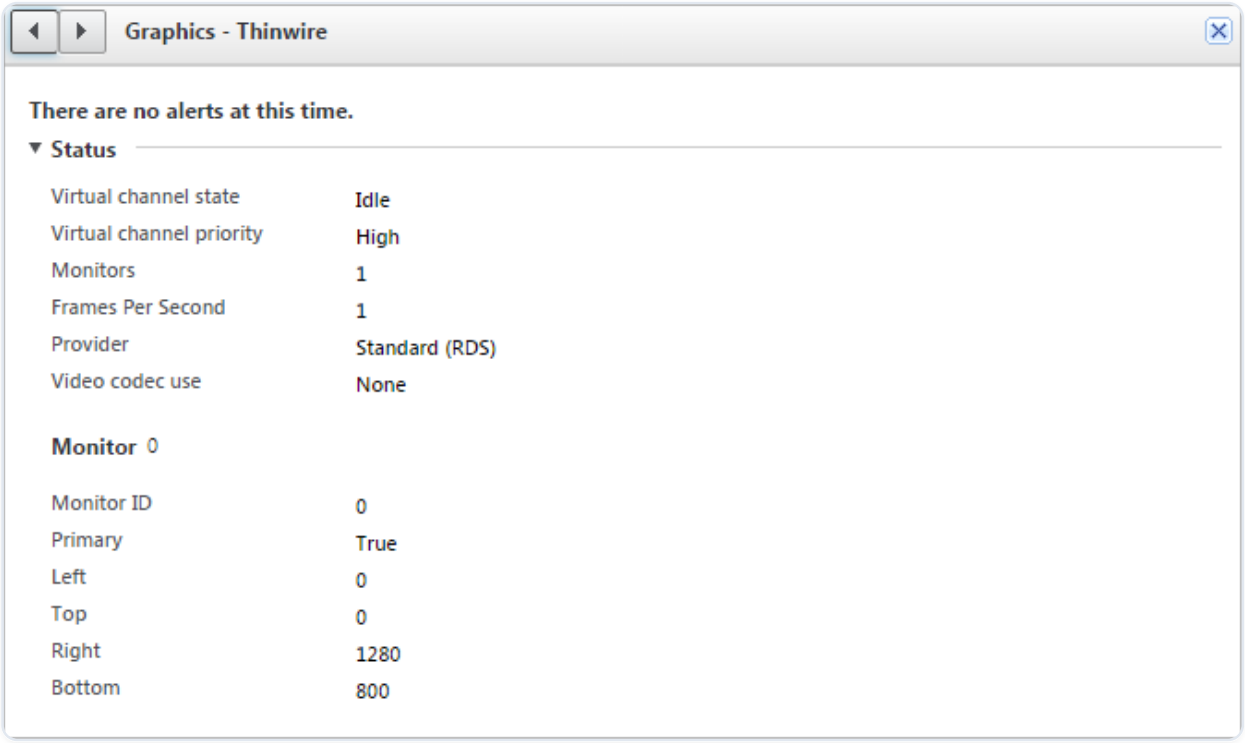
You can monitor the use and performance of Thinwire from Citrix Director. The HDX virtual channel details view contains useful information for troubleshooting and monitoring Thinwire in any session. To view Thinwire-related metrics:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In Director, search for a user, machine or endpoint, open an active session and click **Details**.
   Or, you can select **Filters > Session > All Sessions**, open an active session and click **Details**.
2. Scroll down to the **HDX** panel.



3. Select **Graphics - Thinwire**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lossless compression codec (MDRLE)

In a typical desktop session, most of the imagery is simple graphics or text regions. Thinwire determines where these regions are and selects these areas for lossless encoding using the 2DRLE codec. At the Citrix Workspace app client side, these elements are decoded using the Citrix Workspace app-side 2DRLE decoder for session display.

In XenApp and XenDesktop 7.17, we added a higher compression ratio MDRLE codec that consumes less bandwidth in typical desktop sessions than the 2DRLE codec. This new codec does not impact server scalability.

Lower bandwidth usually means improved session interactivity (especially on shared or constrained links) and reduced costs. For example, the expected bandwidth consumption when using the MDRLE codec is approximately 10–15% less compared with XenApp and XenDesktop 7.15 LTSR for typical Office-like workloads.

Configuration isn't required for the MDRLE codec. If Citrix Workspace app supports MDRLE decoding, the VDA uses the VDA MDRLE encoding and the Citrix Workspace app MDRLE decoding. If Citrix Workspace app doesn't support MDRLE decoding, the VDA automatically falls back to 2DRLE encoding.

MDRLE Requirements:

- Citrix Virtual Apps and Desktops minimum version 7 1808 VDAs
- XenApp and XenDesktop minimum version 7.17 VDAs
- Citrix Workspace app for Windows minimum version 1808
- Citrix Receiver for Windows minimum version 4.11

Progressive Mode

Citrix Virtual Apps and Desktops 1808 introduced progressive mode and enabled it by default. In constrained network conditions (default: bandwidth < 2 Mbps, or latency > 200 ms), Thinwire increased the compression of text and static imagery to improve interactivity during screen activity. The heavily compressed text and images are then progressively sharpened, in a random block fashion, when screen activity stopped. While compressing and sharpening this way improves overall interactivity, it reduces cache efficiency and increases bandwidth usage.

As of Citrix Virtual Apps and Desktops 1906, progressive mode is disabled by default. We now use a different approach. The quality of still images is now based on network conditions and floats between a pre-defined minimum and maximum value for each **Visual quality** setting. Because

© 1997–2026 Citrix Systems, Inc. All rights reserved.

there is no explicit sharpening step, Thinwire optimizes image delivery and maintains cache efficiency, while providing nearly all of the benefits of progressive mode.

Changing progressive mode behavior

You can change the progressive mode state with the registry key. For information, see Progressive mode in the list of features managed through the registry.

H.264 Build to lossless

Build to lossless is a special Thinwire configuration that optimizes graphics delivery for interactivity and final image quality. You can enable this setting by setting the **Visual quality** policy to **Build to lossless**.

Build to lossless compresses the screen using H.264 (or H.265) during screen activity and sharpens to pixel perfect (lossless) when activity stops. The H.264 (or H.265) image quality adapts to available resources to maintain the best possible frame rate. The sharpening step is performed gradually, giving an immediate response if the user begins screen activity shortly after sharpening starts. For example, selecting a model and rotating it.

H.264 **Build to lossless** offers all the advantages of full screen H.264 or H.265, including hardware acceleration, but with the added benefit of a final, guaranteed lossless screen. This is critical for 3D-type workloads that require a final pixel-perfect image. For example, manipulating medical imagery. Also, H.264 **Build to lossless** uses fewer resources than full screen H.264 4:4:4. As a result, using **Build to lossless** usually results in a higher frame rate than Visually lossless H.264 4:4:4.

NOTE:

In addition to the **Visual quality** policy, set the **Use video codec** policy to **Use when preferred** (default) or **For actively changing regions**. You can revert to non-H.264 Build to lossless by setting the **Use video codec** policy to **Do not use video codec**. This results in moving images being encoded with JPEG instead of H.264 (or H.265).

Text-based session watermark

Text-based session watermarks help to deter and enable tracking data theft. This traceable information appears on the session desktop as a deterrent to those using photographs and screen captures to steal data. You can specify a watermark that is a layer of text, which displays over the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

entire session screen without changing the content of the original document. Text-based session watermarks require VDA support.

IMPORTANT:

Text-based session watermarking is not a security feature. The solution does not prevent data theft completely, but it provides some level of deterrent and traceability. Although we do not guarantee complete information traceability when using this feature, we recommend that you combine this feature with other security solutions as applicable.

The session watermark is text and is applied to the session that is delivered to the user. The session watermark carries information for tracking data theft. The most important data is the identity of the logon user of the current session in which the screen image was taken. To trace the data leakage more effectively, include other information such as server or client internet protocol address and a connect time.

To adjust the user experience, use the Session Watermark policy settings to configure the placement and watermark appearance on the screen.

Requirements:

Virtual Delivery Agents:

Multi-session OS 7.17 Single-session OS 7.17

Limitations:

- Session watermarks are not supported in sessions where Local App Access, Windows media redirection, MediaStream, browser content redirection, and HTML5 video redirection are used. To use session watermark, ensure that these features are disabled.
- Session watermark is not supported and doesn't appear if the session is running in full-screen hardware accelerated modes (full-screen H.264 or H.265 encoding).
- If you set these HDX™ policies, watermark settings don't take effect and a watermark isn't displayed in the session display.

Use hardware encoding for video codec to **Enabled Use video codec for compression** to **For the entire screen**

- If you set these HDX policies, the behavior is undetermined and the watermark might not display.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use hardware encoding for video codec to **Enabled Use video codec for compression** to **Use video codec when preferred**

To ensure the watermark displays, set **Use hardware encoding for video codec** to **Disabled**, or set **Use video codec for compression** to **For actively changing regions** or **Do not use video codec**.

- Session watermark supports only the Thinwire graphics mode.
- If you use Session Recording, the recorded session doesn't include the watermark.
- If you use Windows remote assistance, the watermark is not shown.
- If a user presses the **Print Screen** key to capture the screen, the screen captured at the VDA side doesn't include the watermarks. We recommend that you take measures to avoid the captured image being copied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multimedia

The HDX™ technology stack supports the delivery of multimedia applications through two complementary approaches:

- Server-side rendering multimedia delivery
- Client-side rendering multimedia redirection

This strategy ensures that you can deliver a full range of multimedia formats, with a great user experience, while maximizing server scalability to reduce the cost-per-user.

With server-rendered multimedia delivery, audio and video content is decoded and rendered on the Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) server by the application. The content is then compressed and delivered using ICA protocol to Citrix Workspace app on the user device. This method provides the highest rate of compatibility with various applications and media formats. Because video processing is compute-intensive, server-rendered multimedia delivery benefits greatly from the onboard hardware acceleration. For example, support for DirectX Video Acceleration (DXVA) offloads the CPU by performing H.264 decoding in separate hardware. Intel Quick Sync, AMD RapidFire, and NVIDIA NVENC technologies provide hardware-accelerated H.264 encoding.

Because most servers do not offer any hardware acceleration for video compression, server scalability is negatively impacted if all video processing is done on the server CPU. You can maintain high server scalability, by redirecting many multimedia formats to the user device for local rendering.

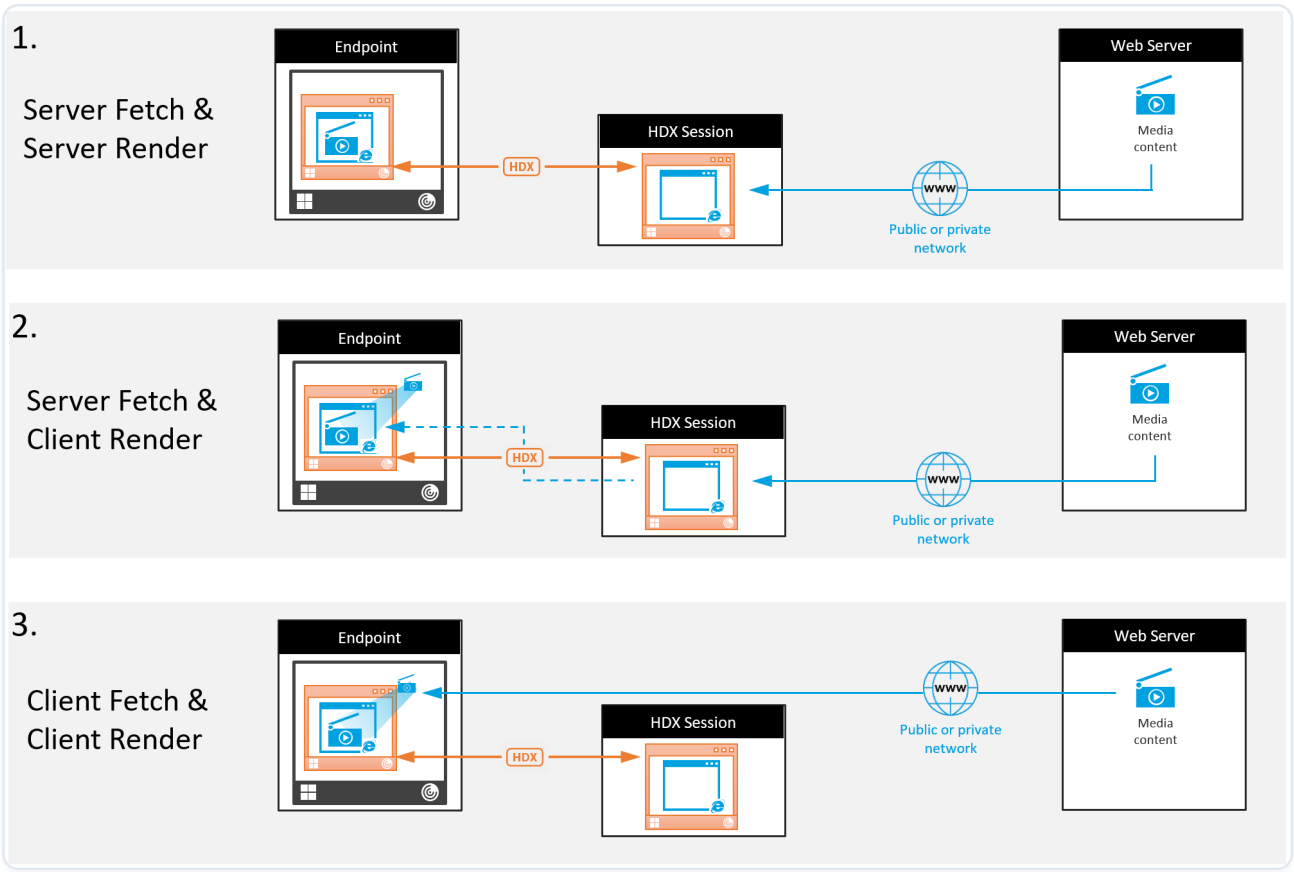
- Windows Media redirection offloads the server for a wide variety of media formats typically associated with the Windows Media Player.
- HTML5 video has become popular, and Citrix® introduced a redirection technology for this type of content. We recommend the browser content redirection for websites using HTML5, HLS, DASH, or WebRTC.
- You can apply the general contact redirection technologies Host-to-client redirection and Local App Access to the multimedia content.

Putting these technologies together, if you don't configure redirection, HDX does Server-Side Rendering. If you configure redirection, HDX uses either Server Fetch and Client Render or Client

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fetch and Client Render. If those methods fail, HDX falls back to Server-Side Rendering as needed and is subject to the Fallback Prevention Policy.

Example scenarios



Scenario 1. (Server Fetch and Server Rendering):

1. The server fetches the media file from its source, decodes, and then presents the content to an audio device or display device.
2. The server extracts the presented image or sound from the display device or audio device respectively.
3. The server optionally compresses it, and then transmits it to the client.

This approach incurs a high CPU cost, high bandwidth cost (if the extracted image/sound isn't compressed efficiently), and has low server scalability.

Thinwire and Audio virtual channels handle this approach. The advantage of this approach is that it reduces the hardware and software requirements for the clients. Using this approach the decoding happens on the server and it works for a wider variety of devices and formats.

Scenario 2. (Server Fetch and Client Render):

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This approach relies on being able to intercept the media content before it is decoded and presented to the audio or display device. The compressed audio/video content is instead sent to the client where it is then decoded and presented locally. The advantage of this approach is that the are offloaded to the client devices, saving CPU cycles on the server.

However, it also introduces some additional hardware and software requirements for the client. The client must be able to decode each format that it might receive.

Scenario 3. (Client Fetching and Client Rendering):

This approach relies on being able to intercept the media content URL before it's fetched from the source. The URL is sent to the client where the media content is fetched, decoded, and presented locally. This approach is conceptually simple. Its advantage is that it saves both CPU cycles on the server and bandwidth because the server sends only control commands. However, the media content is not always accessible to the clients.

Framework and platform:

Single-session operating systems (Windows, Mac OS X, and Linux) provide multimedia frameworks that enable the faster development of multimedia applications. This table lists some of the more popular multimedia frameworks. Each framework divides media processing into several stages and uses a pipelined-based architecture.

FRAMEWORK	PLATFORM
DirectShow	Windows (98 and later)
Media Foundation	Windows (Vista and later)
Gstreamer	Linux
Quicktime	Mac OS X

Double hop support with media redirection technologies

Audio redirection	No
Browser content redirection	No
HDX webcam redirection	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HTML5 Video redirection	Yes
Windows Media redirection	Yes

Audio

You can configure and add the following Citrix policy settings to a policy that optimizes HDX audio features. For usage details plus relationships and dependencies with other policy settings, see Audio policy settings and Bandwidth policy settings and Multi-stream connections policy settings.

IMPORTANT:

We recommend delivering audio using User Datagram Protocol (UDP) rather than TCP. Only Windows Virtual Delivery Agent (VDA) supports audio over UDP.

UDP audio encryption using DTLS is available only between Citrix Gateway and Citrix Workspace™ app. Therefore, sometimes it might be preferable to use TCP transport. TCP supports end-to-end TLS encryption from the VDA to Citrix Workspace app.

Audio quality

In general, higher sound quality consumes more bandwidth and server CPU utilization by sending more audio data to user devices. Sound compression allows you to balance sound quality against overall session performance; use Citrix policy settings to configure the compression levels to apply to sound files.

By default, the **Audio quality policy** setting is set to High - high definition audio when TCP transport is used. The policy is set to Medium - optimized-for-speech when UDP transport (recommended) is used. The **High Definition audio** setting provides high fidelity stereo audio, but consumes more bandwidth than other quality settings. Do not use this audio quality for non-optimized voice chat or video chat applications (such as softphones). The reason being that it might introduce latency into the audio path that is not suitable for real-time communications. We recommend the optimized for speech policy setting for real-time audio, regardless of the selected transport protocol.

When the bandwidth is limited, for example satellite or dial-up connections, reducing audio quality to **Low** consumes the least possible bandwidth. In this situation, create separate policies for users

© 1997–2026 Citrix Systems, Inc. All rights reserved.

on low-bandwidth connections so that users on high-bandwidth connections are not adversely impacted.

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device.

Bandwidth guidelines for audio playback and recording:

- High quality (default)
  - Bitrate: ~100 kbps (min 75, max 175 kbps) for playback / ~70 kbps for microphone capture
  - Number of Channels: 2 (Stereo) for playback, 1 (mono) for microphone capture
  - Frequency: 44100 Hz
  - Bit-depth: 16-bit
- Medium quality (recommended for VoIP)
  - Bitrate: ~16 kbps (min 20, max 40 kbps) for playback, ~16 kbps for microphone capture
  - Number of Channels: 1 (Mono) for both playback and capture
  - Frequency: 16000 Hz (wideband)
  - Bit-depth: 16-bit
- Low quality
  - Bitrate: ~ 11 kbps (min 10; max 25 kbps) for playback, ~11 kbps for microphone capture
  - Number of Channels: 1 (Mono) for both playback and capture
  - Frequency: 8000 Hz (narrowband)
  - Bit-depth: 16-bit

Client audio redirection

To allow users to receive audio from an application on a server through speakers or other sound devices on the user device, leave the **Client audio redirection** setting at **Allowed**. This is the default.

Client audio mapping puts extra load on the servers and the network. However, prohibiting client audio redirection disables all HDX™ audio functionality.

For setting details, see Audio policy settings. Remember to enable client audio settings on the user device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client microphone redirection

To allow users to record audio using input devices such as microphones on the user device, leave the **Client microphone redirection** setting at its default (Allowed).

For security, user devices alert their users when servers they don't trust try to access microphones. Users can choose to accept or reject access before using the microphone. Users can disable this alert on Citrix Workspace app.

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device.

Audio Plug N Play

The Audio Plug N Play policy setting allows or prevents the use of multiple audio devices to record and play sound. This setting is **Enabled** by default. Audio Plug N Play enables audio devices to be recognized. The devices are recognized even if they are not plugged in until after the user session has started.

This setting applies only to Windows Multi-session OS machines.

For setting details, see Audio policy settings.

Audio redirection bandwidth limit and audio redirection bandwidth limit percent

The Audio redirection bandwidth limit policy setting specifies the maximum bandwidth (in kilobits per second) for a playing and recording audio in a session.

The Audio redirection bandwidth limit percent setting specifies the maximum bandwidth for audio redirection as a percentage of the total available bandwidth.

By default, zero (no maximum) is specified for both settings. If both settings are configured, the one with the lowest bandwidth limit is used.

For setting details, see Bandwidth policy settings. Remember to enable Client audio settings on the user device.

Audio over UDP Real-time Transport and Audio UDP port range

By default, Audio over User Datagram Protocol (UDP) Real-time Transport is allowed (when selected at the time of installation). It opens up a UDP port on the server for connections that use Audio over UDP Real-time Transport. If there is network congestion or packet loss, we recommend

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configuring UDP/RTP for audio to ensure the best possible user experience. For any real time audio such as softphone applications, UDP audio is preferred to EDT. UDP allows for packet loss without retransmission, ensuring that no latency is added on connections with high packet loss.

IMPORTANT:

When Citrix Gateway is not in the path, audio data transmitted with UDP is not encrypted. If Citrix Gateway is configured to access Citrix Virtual Apps and Desktops™ resources, then audio traffic between the endpoint device and Citrix Gateway is secured using DTLS protocol.

The Audio UDP port range specifies the range of port numbers that the Windows VDA uses to exchange audio packet data with the user device.

By default, the range is 16500 through 16509.

For setting details about Audio over UDP Real-time Transport, see Audio policy settings. For details about Audio UDP port range, see Multi-stream connections policy settings. Remember to enable Client audio settings on the user device.

Audio over UDP requires the Windows VDA. For supported policies on the Linux VDA, see Policy support list.

Audio setting policies for user devices

1. Load the group policy templates by following Configuring the Group Policy Object administrative template.
2. In the Group Policy Editor, expand **Administrative Templates > Citrix Components > Citrix Workspace > User Experience**.
3. For **Client audio settings**, select **Not Configured**, **Enabled**, or **Disabled**.
   - **Not Configured**. By default, Audio Redirection is enabled using high quality audio or the previously configured custom audio settings.
   - **Enabled**. Enables audio redirection using the selected options.
   - **Disabled**. Disables audio redirection.
4. If you select **Enabled**, choose a sound quality. For UDP audio, use **Medium** (default).
5. For UDP audio only, select **Enable Real-Time Transport** and then set the range of incoming ports to open in the local Windows firewall.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. To use UDP Audio with Citrix Gateway, select **Allow Real-Time Transport Through gateway**. Configure Citrix Gateway with DTLS. For more information, see this article.

As an Administrator, if you do not have control on endpoint devices to make these changes, use the default.ica attributes from StoreFront to enable UDP Audio. For example, for bring your own devices or home computers.

1. On the StoreFront machine, open C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica with an editor such as notepad.
2. Make the following entries under the section.

   ; This text enables Real-Time Transport

   EnableRtpAudio=true

   ; This text allows Real-Time Transport Through gateway

   EnableUDPThroughGateway=true

   ; This text sets audio quality to Medium

   AudioBandwidthLimit=1

   ; UDP Port range

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

If you enable User Datagram Protocol (UDP) audio by editing default.ica, then UDP audio is enabled for all users who are using that store.

Avoid echo during multimedia conferences

Users in audio or video conferences might hear an echo. Echoes usually occur when speakers and microphones are too close to each other. For that reason, we recommend the use of headsets for audio and video conferences.

HDX provides an echo cancellation option (enabled by default) that minimizes any echo. The effectiveness of echo cancellation is sensitive to the distance between the speakers and the microphone. Ensure that the devices aren't too close or too far away from each other.

You can change a registry setting to disable echo cancellation. For information, see Avoid echo during multimedia conferences in the list of features managed through the registry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Softphones

A softphone is software acting as a phone interface. You use a softphone to make calls over the internet from a computer or other smart device. By using a softphone, you can dial phone numbers and carry out other phone-related functions using a screen.

Citrix Virtual Apps and Desktops support several alternatives for delivering softphones.

- **Control mode**. The hosted softphone controls a physical telephone set. In this mode, no audio traffic goes through the Citrix Virtual Apps and Desktops server.
- **HDX RealTime optimized softphone support (recommended)**. The media engine runs on user device, and Voice over Internet Protocol traffic flows peer-to-peer. For examples, see:
  - HDX Optimization for Microsoft Teams
  - HDX RealTime Optimization Pack, which optimizes the delivery of Microsoft Skype for Business
  - Cisco Jabber Softphone for VDI (formerly known as VXME)
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox (formerly known as VDI Communicator)
  - Zoom VDI Plugin
  - Genesys PureEngage Cloud
  - Nuance Dragon PowerMic dictation device
- **Local App Access**. A Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) feature that allows an application such as a softphone to run locally on the Windows user device yet appear seamlessly integrated with their virtual/published desktop. This feature offloads all audio processing to the user device. For more information, see Local App Access and URL redirection.
- **HDX RealTime generic softphone support.** Voice over Internet Protocol-over-ICA.

Generic softphone support

Generic softphone support, enables you to host an unmodified softphone on XenApp or XenDesktop in the data center. The audio traffic goes over the Citrix ICA protocol (preferably using UDP/RTP) to the user device running the Citrix Workspace app.

Generic softphone support is a feature of HDX RealTime. This approach to softphone delivery is especially useful when:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- An optimized solution for delivering the softphone is not available and the user is not on a Windows device where Local App Access can be used.
- The media engine that is needed for optimized delivery of the softphone isn't installed on the user device or isn't available for the operating system version running on the user device. In this scenario, Generic HDX RealTime provides a valuable fallback solution.

There are two softphone delivery considerations using Citrix Virtual Apps and Desktops:

- How the softphone application is delivered to the virtual/published desktop.
- How the audio is delivered to and from the user headset, microphone, and speakers, or USB telephone set.

Citrix Virtual Apps and Desktops include numerous technologies to support generic softphone delivery:

- Optimized-for-Speech codec for fast encode of the real-time audio and bandwidth efficiency.
- Low latency audio stack.
- Server-side jitter buffer to smooth out the audio when the network latency fluctuates.
- Packet tagging (DSCP and WMM) for Quality of Service.
    - DSCP tagging for RTP packets (Layer 3)
    - WMM tagging for Wi-Fi

The Citrix Workspace app versions for Windows, Linux, Chrome, and Mac also are Voice over Internet Protocol capable. Citrix Workspace app for Windows offers these features:

- Client-side jitter buffer - Ensures smooth audio even when the network latency fluctuates.
- Echo cancellation - Allows for greater variation in the distance between microphone and speakers for workers who do not use a headset.
- Audio plug-n-play - Audio devices do not need to be plugged in before starting a session. They can be plugged in at any time.
- Audio device routing - Users can direct ringtone to speakers but the voice path to their headset.
- Multi-stream ICA - Enables flexible Quality of Service-based routing over the network.
- ICA supports four TCP and two UDP streams. One of the UDP streams supports the real-time audio over RTP.

For a summary of Citrix Workspace app capabilities, see Citrix Receiver Feature Matrix.

System configuration recommendations

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client Hardware and Software: For optimal audio quality, we recommend the latest version of Citrix Workspace app and a good quality headset that has acoustic echo cancellation (AEC). Citrix Workspace app versions for Windows, Linux, and Mac support Voice over Internet Protocol. Also, Dell Wyse offers Voice over Internet Protocol support for ThinOS (WTOS).

CPU Considerations: Monitor CPU usage on the VDA to determine if it is necessary to assign two virtual CPUs to each virtual machine. Real-time voice and video are data intensive. Configuring two virtual CPUs reduces the thread switching latency. Therefore, we recommend that you configure two vCPUs in a Citrix Virtual Desktops™ VDI environment.

Having two virtual CPUs does not necessarily mean doubling the number of physical CPUs, because physical CPUs can be shared across sessions.

Citrix Gateway Protocol (CGP), which is used for the Session Reliability feature, also increases CPU consumption. On high-quality network connections, you can disable this feature to reduce CPU consumption on the VDA. Neither of the preceding steps might be necessary on a powerful server.

UDP Audio: Audio over UDP provides excellent tolerance of network congestion and packet loss. We recommend it instead of TCP when available.

LAN/WAN configuration: Proper configuration of the network is critical for good real-time audio quality. Typically, you must configure virtual LANs (VLANs) because excessive broadcast packets can introduce jitter. IPv6-enabled devices might generate many broadcast packets. If IPv6 support is not needed, you can disable IPv6 on those devices. Configure to support Quality of Service.

Settings for use WAN connections: You can use voice chat over LAN and WAN connections. On a WAN connection, audio quality depends on the latency, packet loss, and jitter on the connection. If delivering softphones to users on a WAN connection, we recommend using the NetScaler® SD-WAN between the data center and the remote office. Doing so maintains a high Quality of Service. NetScaler SD-WAN supports Multi-Stream ICA, including UDP. Also, for a single TCP stream, it's possible to distinguish the priorities of various ICA virtual channels to ensure that high priority real-time audio data receives preferential treatment.

Use Director or the HDX Monitor to validate your HDX configuration.

Remote user connections: Citrix Gateway supports DTLS to deliver UDP/RTP traffic natively (without encapsulation in TCP). Open firewalls bidirectionally for UDP traffic over Port 443.

Codec selection and bandwidth consumption: Between the user device and the VDA in the data center, we recommend using the **Optimized-for-Speech** codec setting, also known as Medium

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Quality audio. Between the VDA platform and the IP-PBX, the softphone uses whatever codec is configured or negotiated. For example:

- G711 provides good voice quality but has a bandwidth requirement of from 80 kilobits per second through 100 kilobits per second per call (depending on Network Layer2 overheads).
- G729 provides good voice quality and has a low bandwidth requirement of from 30 kilobits per second through 40 kilobits per second per call (depending on Network Layer 2 overheads).

Delivering softphone applications to the virtual desktop

There are two methods by which you can deliver a softphone to the XenDesktop® virtual desktop:

- The application can be installed in the virtual desktop image.
- The application can be streamed to the virtual desktop using Microsoft App-V. This approach has manageability advantages because the virtual desktop image is kept uncluttered. After being streamed to the virtual desktop, the application runs in that environment as if it was installed in the usual manner. Not all applications are compatible with App-V.

Delivering audio to and from the user device

Generic HDX RealTime supports two methods of delivering audio to and from the user device:

- **Citrix Audio Virtual Channel**. We generally recommend the Citrix Audio Virtual Channel because it's designed specifically for audio transport.
- **Generic USB Redirection**. Supports audio devices having buttons or a display (or both), human interface device (HID), if the user device is on a LAN or LAN-like connection back to the Citrix Virtual Apps and Desktops server.

Citrix audio virtual channel

The bidirectional Citrix Audio Virtual Channel (CTXCAM) enables audio to be delivered efficiently over the network. Generic HDX RealTime takes the audio from the user headset or microphone and compresses it. Then, it sends it over ICA to the softphone application on the virtual desktop. Likewise, the audio output of the softphone is compressed and sent in the other direction to the user headset or speakers. This compression is independent of the compression used by the softphone itself (such as G.729 or G.711). It is done using the Optimized-for-Speech codec (Medium Quality). Its characteristics are ideal for Voice over Internet Protocol. It features quick encode time, and it consumes only approximately 56 Kilobits per second of network bandwidth (28 Kbps in each direction), peak. This codec must be explicitly selected in the service's Manage console because it is not the default audio codec. The default is the HD Audio codec (High

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Quality). This codec is excellent for high fidelity stereo soundtracks but is slower to encode compared to the Optimized-for-Speech codec.

Generic USB Redirection

Citrix Generic USB Redirection technology (CTXGUSB virtual channel) provides a generic means of remoting USB devices, including composite devices (audio plus HID) and isochronous USB devices. This approach is limited to LAN-connected users. This reason being that the USB protocol tends to be sensitive to network latency and requires considerable network bandwidth. Isochronous USB redirection works well when using some softphones. This redirection provides excellent voice quality and low latency. However, Citrix Audio Virtual Channel is preferred because it is optimized for audio traffic. The primary exception is when you're using an audio device with buttons. For example, a USB telephone attached to the user device that is LAN-connected to the data center. In this case, Generic USB Redirection supports buttons on the phone set or headset that control features by sending a signal back to the softphone. There isn't an issue with buttons that work locally on the device.

Limitation

After you install an audio device on your client, enable the audio redirection, and start an RDS session, the audio files might not play audio. As a workaround, add the registry key on the RDS machine, and then restart the machine. For information, see Audio limitation in the list of features managed through the registry.

Browser content redirection

Introduction

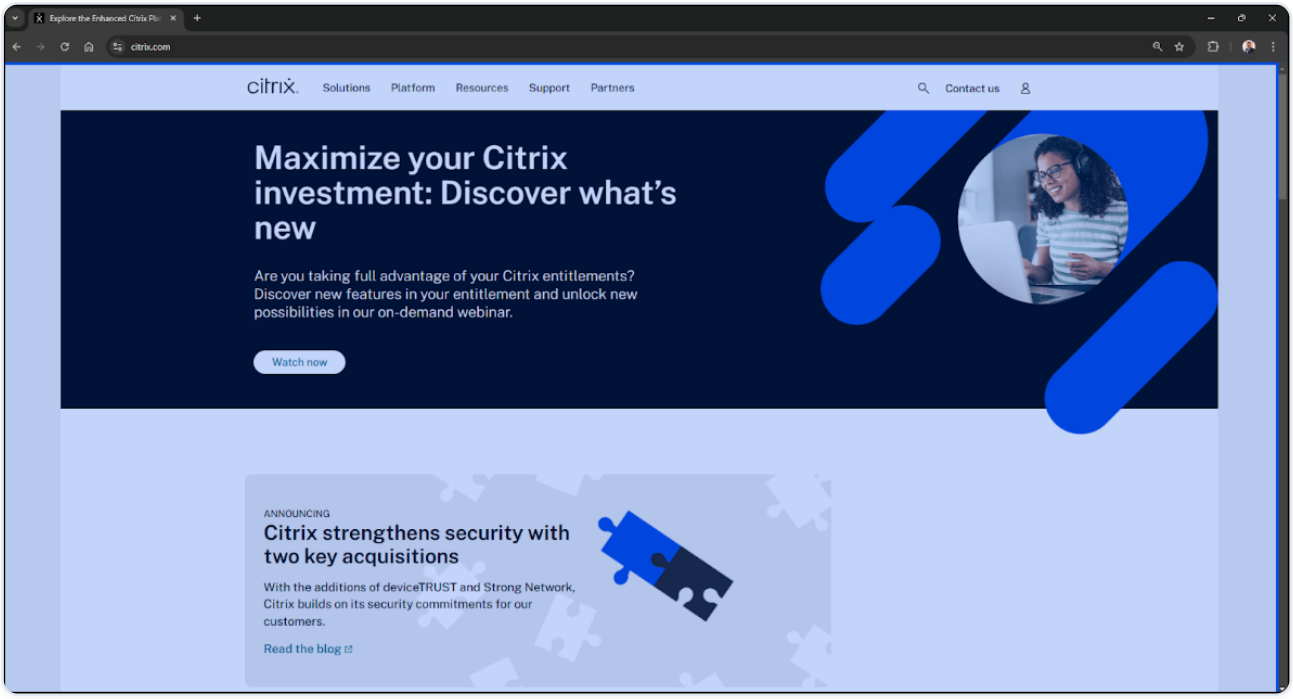
Browser Content Redirection (BCR) enhances the user experience of web browsing within Citrix Virtual Apps and Desktops™ environments. By offloading the rendering of web pages to the user's local machine, BCR reduces server load and improves performance, especially for complex or resource-intensive websites.

How it works

BCR utilizes the Citrix Workspace™ app to create a secure browsing environment on the user's device. When a user accesses an allowed web page, the viewport of the browser window is redirected to the client. The client side browser engine then leverages the local machine's resources to render the page, resulting in faster loading times and smoother interaction.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Note that only the browser viewport is redirected. The viewport is the rectangular area in your browser where the content is displayed. The viewport doesn't include things like the Address Bar, Favorites Toolbar, or Status Bar. Those items are in the user interface, which is still running on the browser in the VDA.



Key Benefits

Browser content redirection intelligently manages the web traffic, delivering a superior experience for your users while reducing strain on your infrastructure.

Here's how they can benefit your organization:

- **Cost Savings:** Offload resource-intensive web pages to user devices, freeing up valuable server resources and reducing bandwidth consumption. This translates to lower hardware and network costs.
- **Enhanced User Experience:** Provide your users with a smoother, more responsive browsing experience, even with graphics-intensive websites. Deliver native-like performance, eliminating lag and improving productivity.
- **Improved Security:** Maintain a secure environment while allowing access to both internal and external resources.
- **Increased Flexibility:** Support a wide range of use cases, from basic web browsing to complex web applications that require proxy traversal or SSO authentication. Easily manage redirection settings with granular policy controls in Citrix Web Studio™

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System Requirements

Server side components

Citrix Virtual Apps and Desktops

- Long Term Service Release
  - Minimum requirements - Any non end-of-life LTSR Citrix Virtual Apps and Desktops release
  - Recommended - Citrix Virtual Apps and Desktops 2402 or above
- Current Release
  - Minimum requirement - Any non end-of-life CR Citrix Virtual Apps and Desktops release
  - Recommended - Latest Citrix Virtual Apps and Desktops release

Browser Components

- Browsers
  - Microsoft Edge
  - Google Chrome
- Browser redirection extension: Published in both Chrome and Edge web stores
- We recommend using the latest version of the browsers for best experience

Client side components

Windows

- Windows 10 or 11
- Citrix Workspace App
  - Minimum Requirement - Any non end-of-life Citrix Workspace App
  - Recommended
    - Long Term Service Release - Citrix Workspace App 2402 latest CU
    - Current Release - Citrix Workspace App 2405 or above

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Browser content redirection is not supported on Citrix Workspace App Windows LTSR releases 1912 and 2203.1
- Client side browser engine needed for Browser content redirection is installed by default on Citrix Workspace App Current Releases
- Client side browser engine needed for Browser content redirection is not installed by default on Citrix Workspace App 2402 LTSR release. Administrators can leverage the ADDLOCAL switch to install BCR browser components on top of Citrix Workspace App.

For more details, please refer to Citrix Workspace App Windows documentation.

Linux

- Citrix Workspace App
  - Minimum requirement - Any non end-of-life Citrix Workspace App
  - Recommended - Citrix Workspace App 2408 or above For more details, please refer to Citrix Workspace App Linux documentation

ChromeOS

- Citrix Workspace App
  - Latest version from Chrome Web Store

MacOS

- Citrix Workspace App
  - Minimum Requirement - Citrix Workspace app 2411 or above

© 1997–2026 Citrix Systems, Inc. All rights reserved.

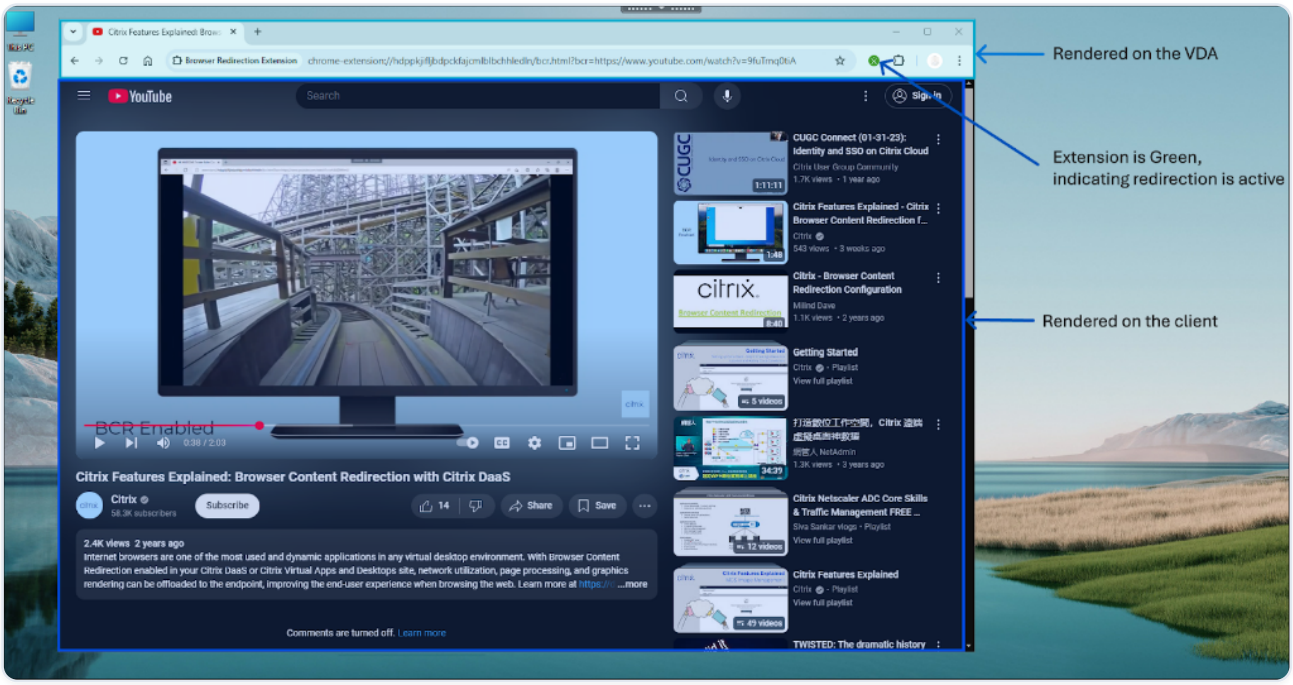
NOTE:

- For MacOS, Browser content redirection package is independent of Citrix Workspace App and is always the latest version. Hence, the package will be compatible with multiple CWA versions above the specified minimum version
- As the dependency on Citrix Workspace App Mac is not there, Browser Content Redirection version numbering will not match Citrix Workspace App Mac version
- Client side browser engine is not packaged with Citrix Workspace App Mac. Download and install the client side for Mac on Citrix Downloads.
- Intel and ARM packages are separate. Hence, you need to install the appropriate version that suits the MacOS endpoint

Steps to Configure

1. Install the client side and server side components according to the system requirements
    - For details on extension deployment, refer Extension deployment section
2. Configure the studio policies
    - Web studio policies offer a granular way to configure Browser content redirection to suit a variety of use cases
    - The basic policies allow the administrator to configure URLs that need to be allowed / not allowed with Browser content redirection
    - The URLs can be configured with wild cards
3. Open a supported web browser and navigate to an allowed URL
    - If the match is found in the allow list, the website will be redirected to the client
    - Citrix Workspace app blends the view port onto the VDA side browser for a seamless experience
4. The color of the extension logo specifies the status of the content redirection
    - Green: Active and Connected
    - Gray: Not active / idle on the current tab
    - Red: Broken / Not Working

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

- HTML5 video redirection and browser content redirection are independent features. The HTML5 video redirection policies aren't needed for this feature to work. However, the Citrix HDX™ HTML5 Video Redirection Service is used for browser content redirection.
- We recommend doing all the configurations through Web Studio and not with registry keys.

Configuration Options

Browser content redirection provides various ways to configure in order to suit the use cases of various customer environments. For detailed information on policy settings, refer Browser content redirection policy settings.

Redirection mechanisms

Client fetch client render

By default, Browser content redirection operates in this mode i.e., the client side browser engine reaches out to the web page directly. This requires necessary access from the client network to the web page. Client fetch client render scenario offloads all the network, CPU and RAM usage from Citrix VDA to the client and is the most optimal way to configure Browser content redirection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLICY CONFIGURATION OPTIONS

- Browser content redirection: Allowed
- Browser content redirection ACL configuration
    - Specify the URLs that need to be redirected. By default, YouTube is the only website configured for redirection
- Browser content redirection block list configuration
    - Optional configuration option to block any specific URLs / sub URLs from redirection. Leverage this option with the above to gain maximum customization.

Server fetch client render

In this case, the client side browser engine contacts and fetches content from the web server through the VDA using a virtual channel. This option is useful when the client doesn't have internet access (for example, thin clients). Low CPU and RAM consumption on the VDA, but bandwidth is consumed on the ICA® virtual channel.

There are three modes of operation in this scenario. The term proxy refers to a proxy device that the VDA accesses to gain Internet access.

POLICY CONFIGURATION OPTIONS

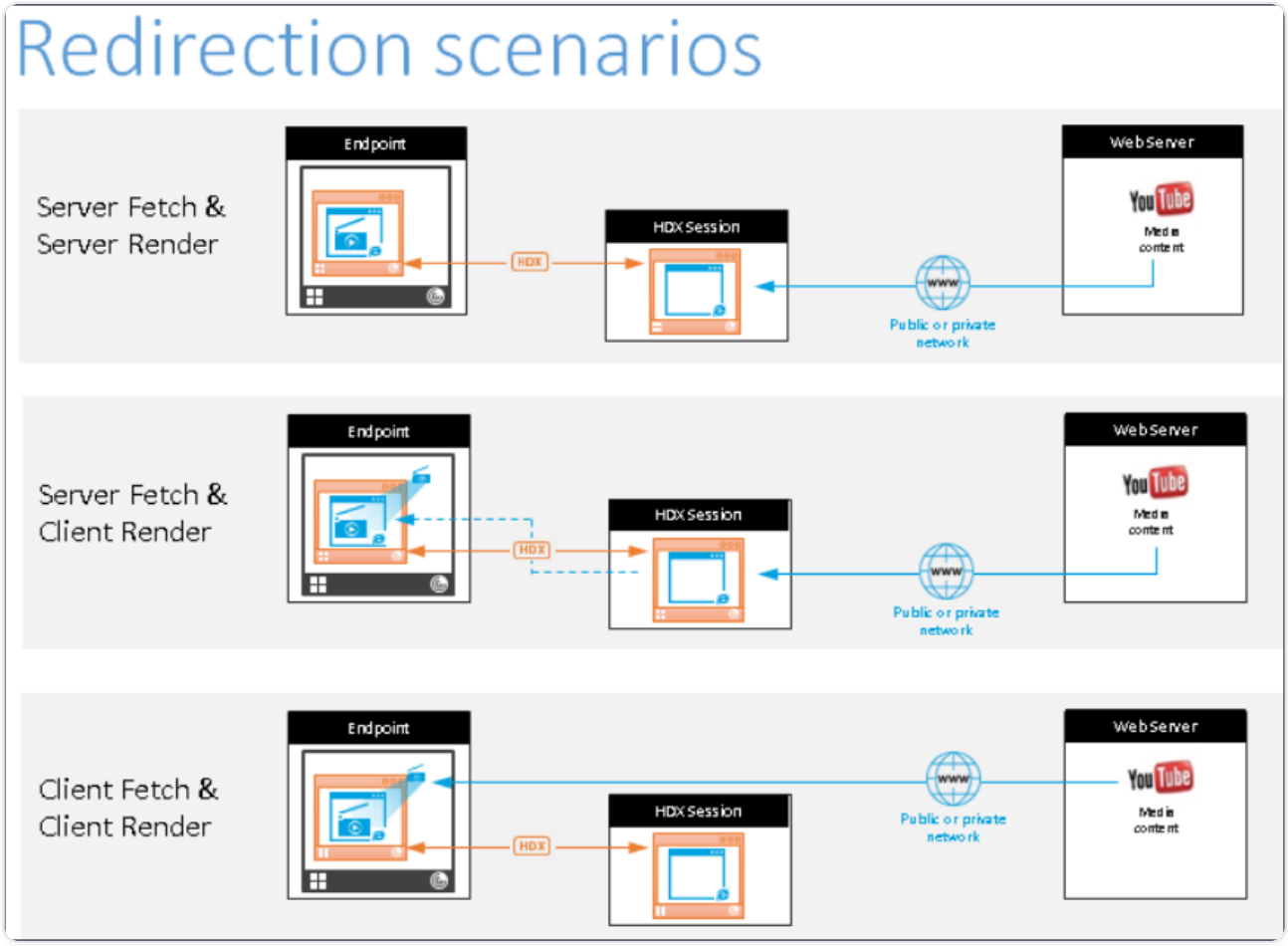
- In addition to the policies specified in the Client fetch client render section, configure the following
- Browser content redirection proxy configuration
    - **Direct or Transparent:** Configure this if you want to leverage server fetch client render and you have direct access or transparent proxy access to the web page from the VDA. The keyword "DIRECT" should be configured in the policy
    - **Explicit Proxy:** Configure this if you want to leverage server fetch client render and you have an explicit proxy access to the web page from the VDA
    - **PAC files:** Configure this if you rely on PAC files browsers in the VDA can automatically choose the appropriate proxy server for fetching a specified URL.

Fallback mode

There might be times when client redirection fails. For example, if the client machine does not have direct internet access, an error response might go back to the VDA. In such cases, the browser on the VDA can then reload and render the page on the server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can suppress server rendering of video elements by using the existing Windows Media fallback prevention policy. Set this policy to Play all content only on client or Play only client-accessible content on client. These settings block video elements from playing on the server if there are failures in client redirection. This policy takes effect only when you enable browser content redirection and the Access Control List policy contains the URL that falls back. The URL can't be in the block list policy.



Authentication handling

Authentication sites

In the current implementation of Browser Content Redirection, regardless of the redirection mechanism, authentication sites need to be configured in order for Browser content redirection to handle log in into websites.

Example:

1. When only https://www.youtube.com/* is configured in Browser content redirection ACL configuration and no authentication sites are configured, BCR will fall back to server side rendering when signing into the website and will continue there.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. In this case, in order for BCR to handle authentication sites, configure https://www.accounts.google.com/* and any other auth sites such as IdP website as needed. Each website sign in works differently and hence ensure to list
3. When configured, BCR will handle the authentication. For example, with client fetch client render - the authentication will also happen from the client side browser engine for a seamless sign in experience.

POLICY CONFIGURATION OPTIONS

Configure the Browser content redirection authentication sites policy in addition to the policies mentioned in the redirection mechanisms section

NOTE:

- BCR client side browser does not persist cookies (including authentication) after the redirected window is closed. This would manifest as the need to re-login into websites when BCR windows are completely closed and re-opened.
- BCR client side browser does not read cookies from the VDA side browser. Hence, user personalization and preferences don't synchronize with the VDA browser.

Integrated Windows Authentication

Browser content redirection can provide a seamless way to authenticate to websites when configured with Integrated Windows Authentation (IWA) within the same domain as the VDA.

POLICY CONFIGURATION OPTIONS

- Configure the Browser content redirection Integrated Windows Authentication support policy

Before enabling single sign-on, complete the following:

- Configure the Kerberos infrastructure to issue tickets for service principal names (SPNs) constructed from the host name. For example, HTTP/serverhostname.com.
- For server fetch client render: When you use browser content redirection in server fetch mode, ensure that DNS is configured properly on the VDA.
- For client fetch client render: When you use browser content redirection in client fetch mode, ensure that DNS is configured properly on the client device and that you allow TCP connections from the overlay to the web server's IP address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Proxy Authentication

Browser content redirection can provide a seamless way to authenticate to your web proxy when fetching content from the server. When enabled, Browser Content Redirection will automatically obtain and use a Kerberos service ticket to authenticate with the proxy

POLICY CONFIGURATION OPTIONS

- Configure the Browser content redirection Server fetch proxy auth policy

Before enabling the server fetch proxy auth policy, complete the following:

- You need to configure your PAC file to route traffic through a downstream web proxy and set up the proxy to use Kerberos authentication

Use Cases

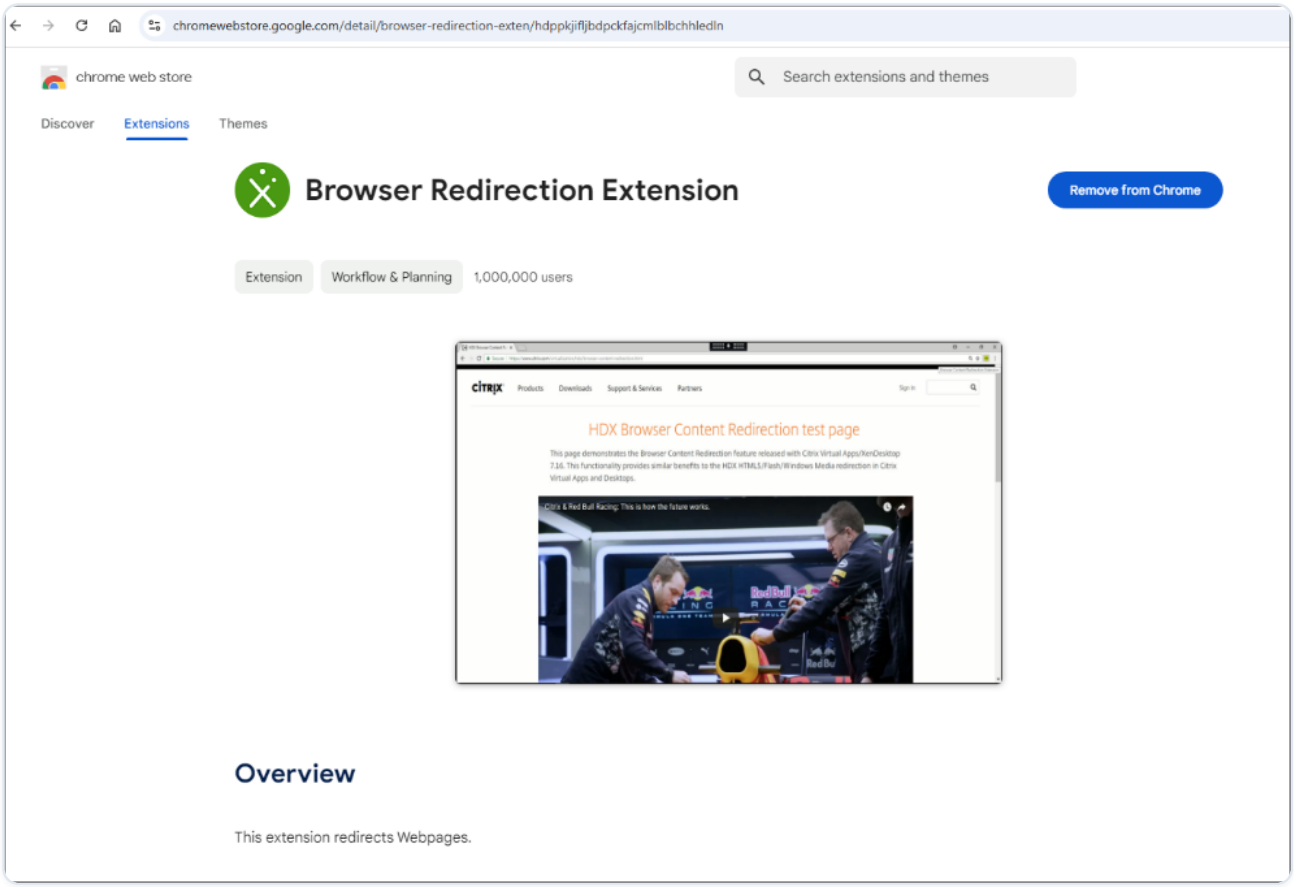
Browser Content Redirection (BCR) can be utilized for a wide range of websites, particularly those that are resource-intensive and frequently accessed by enterprises. This includes video streaming platforms like YouTube, which can significantly benefit from offloading rendering to endpoint devices, thereby reducing server load and saving costs. Additionally, BCR is ideal for unified communications applications, such as video conferencing and collaboration tools (Google meet, Teams web, Zoom web) and contact center applications (Genesys cloud), ensuring smooth performance and enhanced user experience. By leveraging BCR, enterprises can optimize their resources and improve efficiency across various web-based applications. Refer CTX238236 for information on how to configure specific websites.

Extension Deployment

Deploy Manually

Browser redirection extension is published in Chrome and Edge web stores. The extension is needed only on the browser on the VDA and not on the client side. To install the extension, navigate to Chrome / Edge webstore, search for Browser redirection extension and Add to the respective browsers. This method works for individual users. To deploy the extension to a large group of users, deploy the extension using group policy

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Deploy Using Group Policy

PREREQUISITES

- **Access:** You'll need administrator privileges on the machine or within your Active Directory environment where you'll be configuring Group Policy.
- **ADMX Files:** Download the Google Chrome ADMX files (administrative templates) for your version of Chrome. You can find these on the Google Chrome Enterprise Help page.
- **Edge Templates:** Download the Microsoft Edge administrative templates (ADMX files) from the Microsoft Edge Enterprise landing page.
- **Extension ID and Update URL:** The extension ID and update URL for the Citrix Browser Content Redirection extension.

STEPS FOR GOOGLE CHROME

1. Import ADMX Files:
    - Copy the Chrome ADMX files to your central store for administrative templates. This is typically %SystemRoot%\PolicyDefinitions on your domain controller.
2. Open Group Policy Management:
    - Launch the Group Policy Management Console (gpmc.msc).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Create or Edit a GPO:
    - Either create a new Group Policy Object (GPO) or edit an existing one that applies to the users or computers where you want to deploy the extension.
4. Navigate to Extensions Settings:
    - In the GPO editor, go to:
        - User Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Google > Google Chrome > Extensions
5. Enable "Configure the list of force-installed apps and extensions":
    - Double-click this policy setting and select "Enabled."
    - If the Configure the list of force-installed apps and extensions setting is set to Disabled, the extension is automatically removed from Chrome for all users.
6. Add the Extension ID and Update URL:
    - Click the "Show" button.
    - Enter the extension ID and update URL in the format: <extension_id>;<update_url>
    - Value: hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx (Update URL)
7. Apply the GPO:
    - Link the GPO to the appropriate Organizational Unit (OU) in your Active Directory structure.
8. Update Group Policy:
    - On the target machines, run gpupdate /force to apply the policy immediately, or wait for the policy to update automatically.

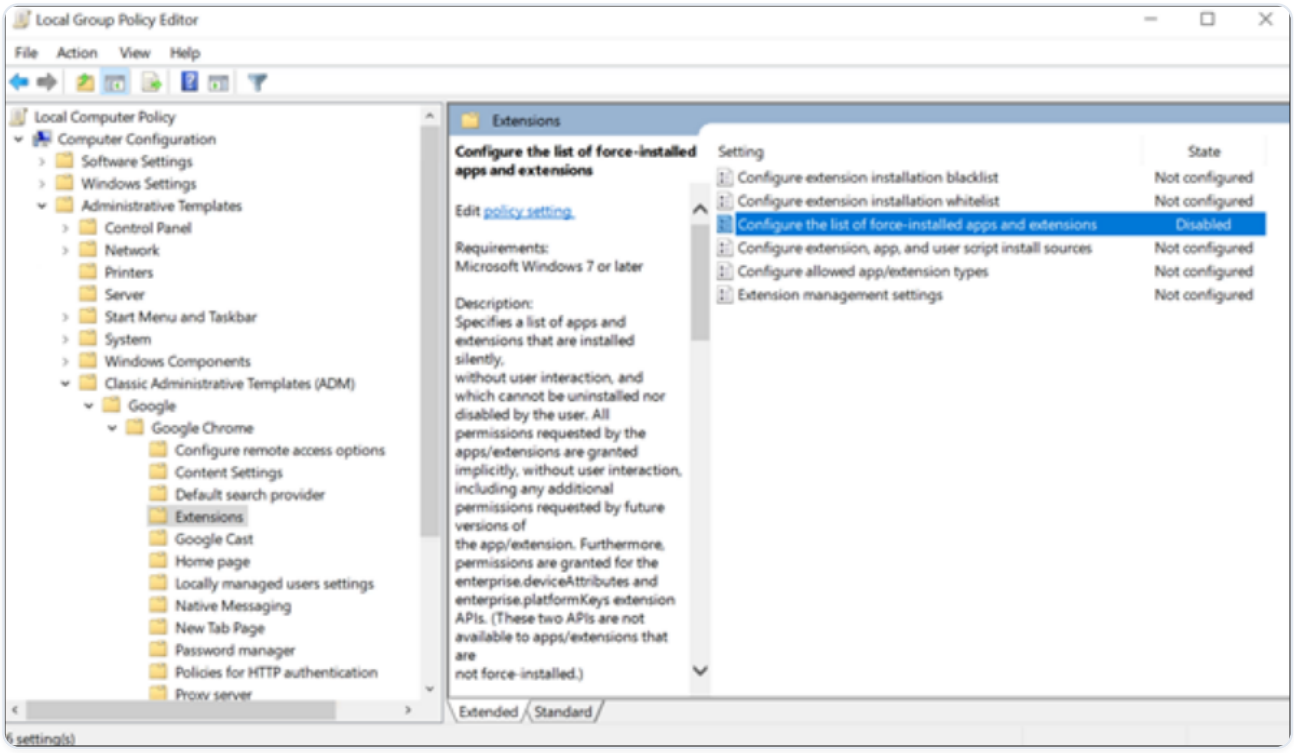
STEPS FOR MICROSOFT EDGE

1. Import ADMX Files:
    - Copy the Edge ADMX files to your central store for administrative templates (%SystemRoot%\PolicyDefinitions).
2. Open Group Policy Management:
    - Launch the Group Policy Management Console (gpmc.msc).

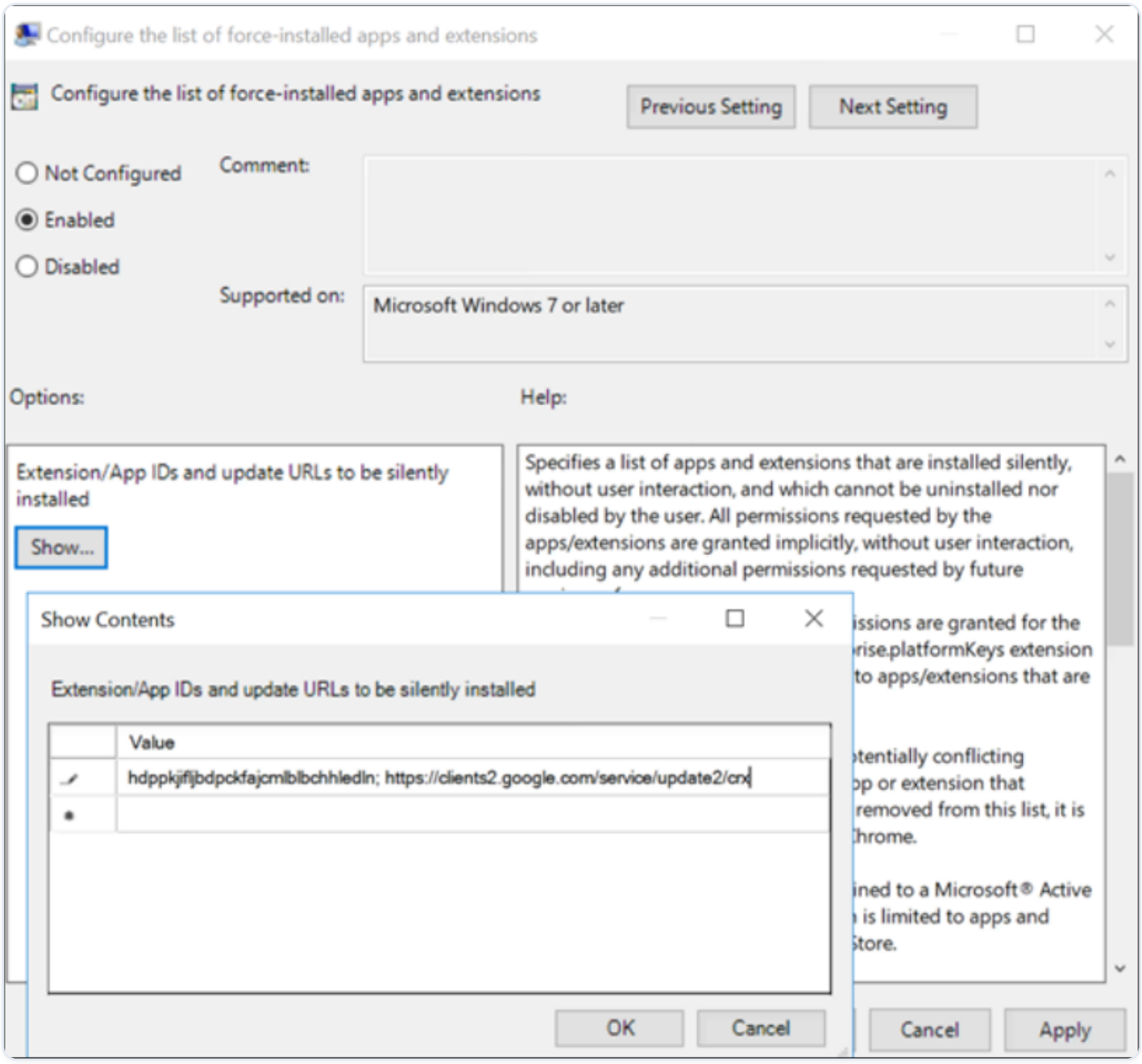
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Create or Edit a GPO:
    - Create a new GPO or edit an existing one.
4. Navigate to Extensions Settings:
    - In the GPO editor, go to:
        - Computer Configuration > Policies > Administrative Templates > Microsoft Edge > Extensions
5. Enable "Control which extensions are installed silently":
    - Double-click this policy setting and select "Enabled."
6. Add the Extension ID and Update URL:
    - Click the "Show" button.
    - Enter the extension ID and update URL in the format: <extension_id>;<update_url>
    - Value: hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx (Update URL)
7. Apply the GPO:
    - Link the GPO to the appropriate Organizational Unit (OU) in your Active Directory structure.
8. Update Group Policy:
    - On the target machines, run gpupdate /force or wait for the automatic update.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Troubleshooting

For troubleshooting information, see the How to troubleshoot browser content redirection knowledge center article.

Browser Content Redirection Limitations

Server side limitations (VDA)

Browser content redirection cannot support the following use cases. In case an enhancement is required for any mentioned scenarios or new scenarios, please reach out to the Citrix product team.

- Pop-up windows are not supported with Browser content redirection.
- Session cookie persistence is not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HTML5 video redirection policy must be disabled with Browser content redirection is in use.
- In scenarios of session disconnect / reconnect, the VDA browser window needs to be refreshed in order for BCR to kick in again.
- Printing and file downloads from BCR'ed windows are not supported.
- Incognito or private browsing mode is not supported with Browser content redirection.

Client side limitations (CWA)

- Browser content redirection is not supported on ARMhf framework
- BCR supports a maximum of 25 redirected tabs on one browser and a combined 30 redirected tabs in two browsers.

HDX™ video conferencing and webcam video compression

WARNING:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Webcams can be used by applications running within the virtual session by using HDX webcam video compression or HDX plug-n-play generic USB redirection. Use **Citrix Workspace™ app > Preferences > Devices** to switch between modes. Citrix recommends you always use HDX webcam video compression if possible. HDX generic USB redirection is recommended only when there are application compatibility issues with HDX video compression or when you require advanced native functionalities of the webcam. For better performance, Citrix recommends the Virtual Delivery Agent to have at least two virtual CPUs.

To prevent users from switching from HDX webcam video compression, disable USB device redirection by using the policy settings under **ICA® policy settings > USB Devices policy** settings. Citrix Workspace app users can override the default behavior by choosing the Desktop Viewer Mic & Webcam setting **Don't use my microphone or webcam**.

HDX webcam video compression

HDX webcam video compression is also called **Optimized** webcam mode. This type of webcam video compression sends the H.264 video directly to the video conferencing application running in

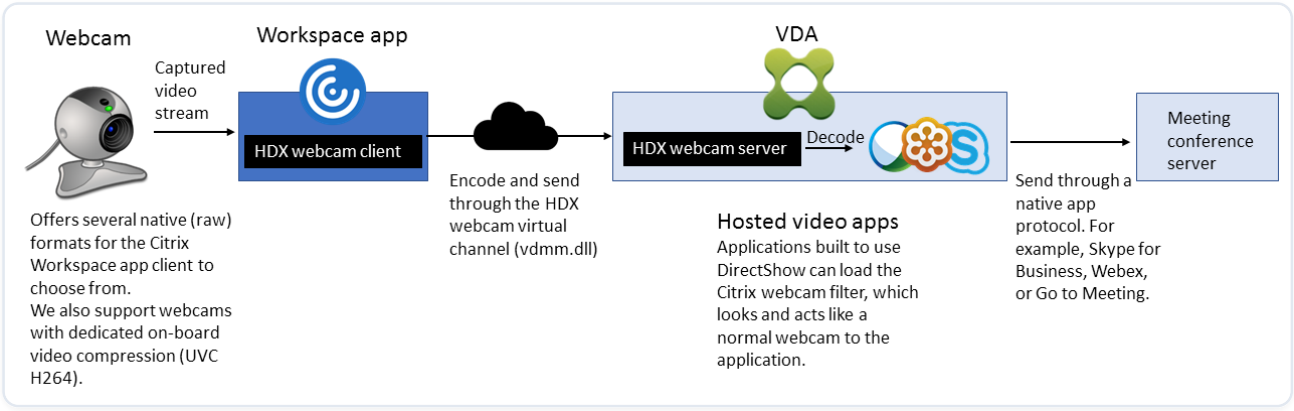
© 1997–2026 Citrix Systems, Inc. All rights reserved.

the virtual session. To optimize VDA resources, HDX webcam compression doesn't encode, transcode, and decode webcam video. This feature is enabled by default.

To disable direct video streaming from the server to the video conferencing app, set the registry key to 0 on the VDA. For information, see Webcam video compression in the list of features managed through the registry.

If you disable the default functionality for streaming video resources, HDX webcam video compression uses the multimedia framework technology that is part of the client operating system to intercept video from capture devices, transcode, and compress it. Manufacturers of capture devices supply the drivers that plug into the OS kernel streaming architecture.

The client handles communication with the webcam. The client then sends the video only to the server that can display it properly. The server doesn't deal directly with the webcam, but its integration gives you the same experience in your desktop. Workspace app compresses the video to save bandwidth and provide better resiliency on WAN scenarios.



HDX webcam video compression requires that the following policy settings be enabled (all are enabled by default).

- Multimedia conferencing
- Windows Media Redirection

If a webcam supports hardware encoding, HDX video compression uses the hardware encoding by default. Hardware encoding might consume more bandwidth than software encoding. To force software compression, edit the registry key on the client. For information, see Webcam software compression in the list of features managed through the registry.

HDX webcam video compression requirements

HDX webcam video compression supports the following versions of Citrix Workspace app:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PLATFORM	PROCESSOR
Citrix Workspace app for Windows	Citrix Workspace app for Windows supports webcam video compression for 32-bit and 64-bit apps on XenApp and XenDesktop 7.17 and later. On earlier versions, Citrix Workspace app for Windows supports only 32-bit apps.
Citrix Workspace app for Mac	Citrix Workspace app for Mac 2006 or later supports webcam video compression for 64-bit apps on XenApp and XenDesktop 7.17 and later. On earlier versions, Citrix Workspace app for Mac supports only 32-bit apps.
Citrix Workspace app for Linux	Citrix Workspace app for Linux supports only 32-bit apps on the virtual desktop.
Citrix Workspace app for Chrome	Because some ARM Chromebooks don't support H.264 encoding, only 32-bit apps can use the optimized HDX webcam video compression.

Media foundation-based video applications support HDX webcam video compression on Windows 8.x or higher and Windows Server 2012 R2 and higher. For more information, see Knowledge Center article CTX132764.

Other user device requirements:

- Appropriate hardware to produce sound.
- DirectShow-compatible webcam (use the webcam default settings). Webcams that are hardware encoding capable reduce client-side CPU usage.
- For HDX webcam video compression, install webcam drivers on the client, obtained from the camera manufacturer, if possible. Installation of the device drivers isn't required on the server.

Different webcams offer different frame rates and have different levels of brightness and contrast. Adjusting the contrast of the webcam can reduce upstream traffic significantly. Citrix uses the following webcams for initial feature validation:

- Microsoft LifeCam VX models (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Logitech C600, C920
- HP Deluxe Webcam

To adjust the preferred video frame rate, edit the registry key on the client. For information, see Webcam video compression frame rate in the list of features managed through the registry.

High-definition webcam streaming

The video conferencing application on the server selects the webcam format and resolution based on the supported format types. When a session starts, the client sends the webcam information to the server. Choose a webcam from the application. When the webcam and the video conferencing application support high-definition rendering, the application uses high-definition resolution. We support webcam resolutions up to 1920x1080.

This feature requires the Citrix Workspace app for Windows, minimum version 1808 or Citrix Receiver for Windows, minimum version 4.10.

You can use a registry key to disable and enable the feature. For information, see High-definition webcam streaming in the list of features managed through the registry.

If the media type negotiation fails, HDX falls back to the default resolution of 352x288 CIF. You can use registry keys on the client to configure the default resolution. Ensure that the camera supports the specified resolution. For information, see High-definition webcam resolution in the list of features managed through the registry.

HDX webcam video compression uses significantly less bandwidth compared to plug-n-play generic USB redirection and works well over WAN connections. To adjust the bandwidth, set the registry key on the client. For information, see High-definition webcam bandwidth in the list of features managed through the registry.

Enter a value in bits per second. If you don't specify the bandwidth, the video conferencing applications use 350000 bps by default.

HDX plug-n-play generic USB redirection

HDX plug-n-play generic USB redirection (isochronous) is also called **Generic** webcam mode. The benefit of HDX plug-n-play generic USB redirection is that you don’t have to install drivers on your thin client/endpoint. The USB stack is virtualized such that anything you plug into the local client is sent to the remote VM. The remote desktop acts as if you plugged it in natively. The Windows desktop handles all the interaction with the hardware and runs through the plug-n-play logic to find the correct drivers. Most webcams work if the drivers exist on the server and can work over ICA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Generic webcam mode uses significantly more bandwidth (many Megabits per second) because you are sending uncompressed video down with USB protocol over the network.

HTML5 multimedia redirection

HTML5 multimedia redirection extends the multimedia redirection features of HDX™ MediaStream to include HTML5 audio and video. Because of growth in online distribution of multimedia content, especially to mobile devices, the browser industry has developed more efficient ways to present audio and video.

Flash has been the standard, but it requires a plug-in, doesn't work on all devices, and has higher battery usage in mobile devices. Companies like YouTube, NetFlix.com, and newer browsers versions of Mozilla, Google, and Microsoft are moving to HTML5 making it the new standard.

HTML5-based multimedia has many advantages over proprietary plug-ins, including:

- Company-independent standards (W3C)
- Simplified digital rights management (DRM) workflow
- Better performance without the security issues raised by plug-ins

HTTP progressive downloads

HTTP progressive download is an HTTP-based pseudo-streaming method that supports HTML5. In a progressive download, the browser plays back a single file (encoded at a single quality) while it is being downloaded from an HTTP web server. The video is stored on the drive as it's received and is played from the drive. If you rewatch the video, the browser can load the video from cache.

For an example of a progressive download, see the HTML5 video redirection test page. To inspect the video elements in the webpage and find the sources (mp4 container format) in HTML5 video tags, use the developer tools in your browser:

Comparing HTML5 and Flash

FEATURE	HTML5	FLASH
Requires a proprietary player	No	Yes
Runs on mobile devices	Yes	Some
Running speed on different platforms	High	Slow

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	HTML5	FLASH
Supported by iOS	Yes	No
Resource usage	Less	More
Load faster	Yes	No

Requirements

We support only redirection for progressive downloads in mp4 format. We don't support WebM and Adaptive bitrate streaming technologies like DASH/HLS.

We support the following, and use policies to control them. For more information, see Multimedia policy settings.

- Server side render
- Server fetch client render
- Client side fetching and rendering

Minimum versions of Citrix Workspace™ app and Citrix Receiver™:

- Citrix Workspace app 1808 for Windows
- Citrix Receiver for Windows 4.5
- Citrix Workspace app 1808 for Linux
- Citrix Receiver for Linux 13.5

MINIMUM VDA BROWSER VERSION	WINDOWS OS VERSION/BUILD/SP
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) and x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Firefox 47 Manually add the certificates to the Firefox certificate store or configure Firefox to search for certificates from a Windows trusted certificate store. For more information, see `https://wiki.mozilla.org/CA:AddRootToFirefox`	Windows 10 x86 (1607 RS1) and x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MINIMUM VDA BROWSER VERSION	WINDOWS OS VERSION/BUILD/SP
Chrome 51	Windows 10 x86 (1607 RS1) and x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

Components of the HTML5 video redirection solution

- **HdxVideo.js** - JavaScript hook intercepting video commands on the website. HdxVideo.js communicates with WebSocketService using Secure WebSockets (SSL/TLS).
- **WebSocket SSL Certificates**
  - For the CA (root): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA) Location: Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates.
  - For the end-entity (leaf): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service) Location: Certificates (Local Computer) > Personal > Certificates.
- **WebSocketService.exe** - Runs on the local system and performs SSL termination and user session mapping. TLS Secure WebSocket listening on 127.0.0.1 port 9001.
- **WebSocketAgent.exe** - Runs on the user session and renders the video as instructed from WebSocketService commands.

How do I enable HTML5 video redirection?

In this release, this feature is available for controlled webpages only. It requires the addition of the HdxVideo.js JavaScript (included in the Citrix Virtual Apps and Desktops Installation media) to the webpages where the HTML5 multimedia content is available. For example, videos on an internal training site.

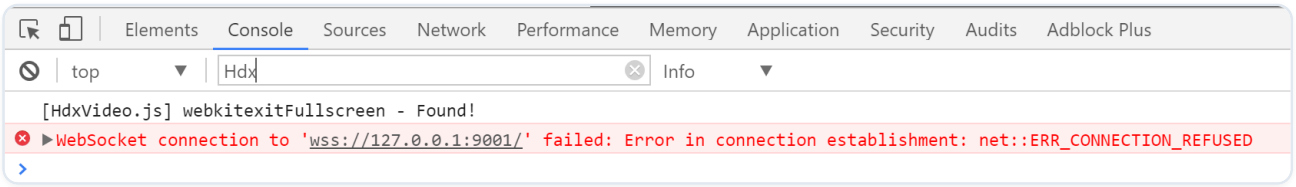
Websites like youtube.com, which are based on Adaptive Bitrate technologies (for example, HTTP Live Streaming (HLS) and Dynamic Adaptive Streaming over HTTP (DASH)), are not supported.

For more information, see *Multimedia policy settings*.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting Tips

Errors might occur when the webpage tries to run HdxVideo.js. If the JavaScript fails to load, the HTML5 redirection mechanism fails. Ensure that there are no errors related to HdxVideo.js by inspecting the console in the developers tool windows of your browser. For example:



Optimization for Microsoft Teams (New)

Citrix® supports two ways to optimize Microsoft Teams audio and video in a VDI environment: Citrix HDX™ Optimization and the New VDI solution for Teams from Microsoft. Classic Teams has reached end of life, so the optimization approaches described on this page apply to the current Microsoft Teams client.

NOTE:

Microsoft has announced the deprecation of WebRTC-based Citrix HDX Optimization for Microsoft Teams on Windows endpoints. Two milestones apply:

- October 1, 2026 - End of Support: No longer officially supported by Microsoft or Citrix.
- April 1, 2027 - End of Availability: WebRTC-based optimization stops functioning. Citrix Studio policies for the legacy optimization no longer take effect.

Customers are recommended to migrate to the New VDI solution for Teams. This change affects Windows endpoints only. macOS, Linux, ChromeOS, and HTML5 endpoints are not impacted. For more details, see Microsoft Blog.

Optimization approaches

- **Citrix HDX Optimization (MTOP)**: A combined Citrix and Microsoft solution that uses a Citrix-owned virtual channel (CTXMTOP). Media offloading is handled by `HdxRtcEngine` in the Citrix Workspace™ app. This solution is traditionally referred to as MTOP.
- **New VDI solution for Teams**: A newer optimization that is owned and managed by Microsoft and uses Microsoft-owned virtual channels (MSTEAMS, MSTEAM1, and MSTEAM2). It is available on Windows and Mac endpoints. For full details, see New VDI solution for Teams in the Microsoft documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Key distinctions

CITRIX HDX OPTIMIZATION	NEW VDI SOLUTION FOR TEAMS
Optimization is a combined solution of Citrix and Microsoft and uses a virtual channel owned by Citrix (CTXMTOP).	Optimization solution is owned and managed by Microsoft and uses virtual channels owned by Microsoft (MSTEAMS, MSTEAM1, and MSTEAM2).
Media offloading is handled by `HdxRtcEngine` which resides in Citrix Workspace app.	Media offloading is handled by the SlimCore media engine on Windows and Mac endpoints.
No additional components needed on the endpoint except installation of Citrix Workspace app.	Additional component - **Teams VDI Plugin** needs to be deployed on the endpoint through various means. This plug-in manages the download and updates of the SlimCore media engine.
Available on endpoint platforms - Windows, macOS, Linux, and ChromeOS.	Available on endpoint platforms - Windows and Mac.
New features are managed in conjunction between Citrix and Microsoft.	New features are managed by Microsoft. Users have access to some new features unavailable with Citrix HDX Optimization.
Supported by both Citrix and Microsoft, depending on the component involved. Customers can open a case with either Citrix or Microsoft and are redirected to the appropriate team as needed.	Owned and supported by Microsoft. Citrix supports the Citrix components involved, such as Citrix Workspace app, the virtual channel allow list, and plug-in deployment mechanisms.

Interoperability and roaming

Citrix HDX Optimization and the New VDI solution for Teams can exist in parallel, but the Teams client uses only one of them at a time.

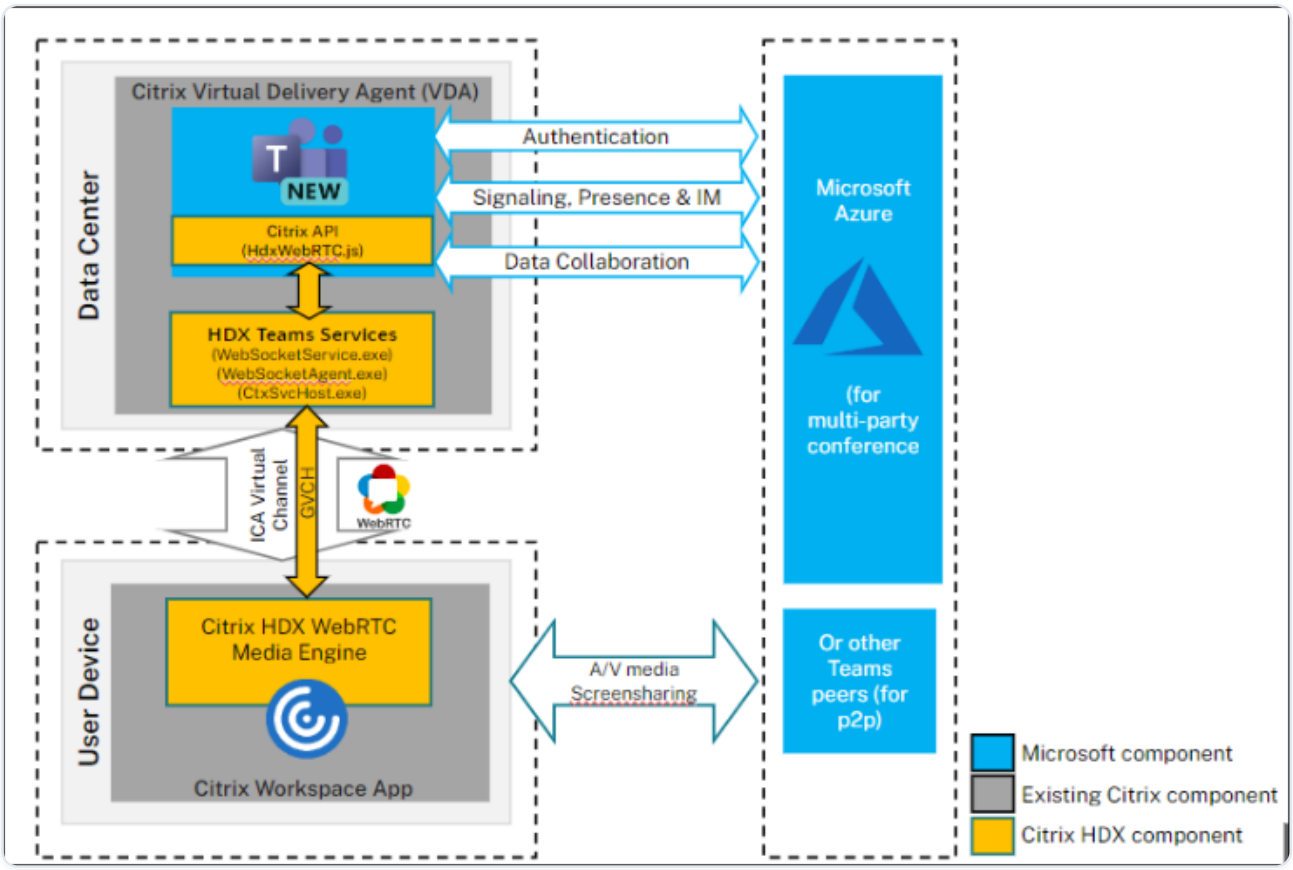
- The optimization is selected when the Teams app launches, in the following order: New VDI solution for Teams, then Citrix HDX Optimization (WebRTC), then standard audio/video redirection.
- If the New VDI solution for Teams fails, Teams falls back directly to standard audio/video redirection rather than to WebRTC. A Teams app restart is required to re-run the selection and choose the optimization that fits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Roaming between endpoints is seamless and does not require a Teams app restart, including when a user roams between an endpoint that supports the New VDI solution for Teams and one that does not.

Citrix HDX™ Optimization

In Citrix HDX (WebRTC Optimization), the media engine (HdxRtcEngine) on the endpoint responsible for handling offloaded media is embedded in the Citrix Workspace™ app and installing the Citrix Workspace app automatically installs the engine as well.



System requirements

This section depicts the minimum and recommended versions necessary to support the new Teams client. Note that in minimum versions some critical bug fixes or latest features might not be available. Deploy the recommended versions to have the best experience with the latest fixes and features.

VDI operating systems

For detailed information, see the recommendations provided in the Microsoft documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Windows Server 2016 is not supported. Citrix recommends you to plan your upgrades accordingly.
- As versions are updated frequently, the versions mentioned here might become end-of-life. Hence, see the product lifecycle pages of Citrix Workspace app and Citrix Virtual Apps and Desktops to ensure you're using supported versions of different components.
- If you're on Citrix Virtual Apps and Desktops™ 1912 LTSR, Citrix recommends planning an upgrade as it'll be end of life in December of 2024.

Virtual Delivery Agent (VDA)

MINIMUM VERSIONS	RECOMMENDED VERSIONS
1912 LTSR CU8+; 2203 LTSR (any CU); 2212 CR	2203 LTSR CU5+ (or) 2402 LTSR and any CR versions above

Citrix Workspace app

MINIMUM VERSIONS	RECOMMENDED VERSIONS
Windows 2203 LTSR (latest CU); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/ HTML5 2301	Windows 2402 LTSR; Windows 2405 CR; Linux 2405; Mac 2405; ChromeOS/HTML5 2405

Deployment

1. Install the new Teams client on VDI. For detailed information, see Deploy new Teams for VDI.
2. Configure the following registry key on the VDA to optimize new Teams.
   - **Location**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **Key (REG_Multi_SZ)**: `ProcessWhitelist`
   - **Value**: `msedgewebview2.exe`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Starting with Citrix Virtual Apps and Desktops 2402 LTSR (or) Citrix Virtual Apps and Desktops 2203 LTSR CU5+, you don't need to manually configure the `msedgewebview2.exe` registry entry as it's allow-listed by default.

3. Ensure that the Microsoft Teams redirection policy is enabled. This policy is turned on by default.
4. No additional configuration is needed on the client side. Follow the wizard instructions to install the Citrix Workspace app.

App Layering

New Microsoft Teams has changed its installation method and now installs under C:\Program Files\WindowsApps. To support this change, you must run App Layering version 2403.2 or later. You can download an upgrade disk in the App Layering downloads page that includes this fix.

For detailed information, see the App Layering documentation.

Citrix Profile Management

See the Citrix Profile Management documentation for information on how to enable roaming for New Microsoft Teams. Current minimum version guidance for Citrix Profile Management is 2402 LTSR (or) 2203 LTSR CU5+.

Networking considerations

Networking requirements for New Teams don't differ from Classic Teams. Hence, see the Network Requirement section in Classic Teams documentation.

Feature matrix and version support

As versions are updated frequently, some older versions mentioned here might reach end of life. Hence, see the product lifecycle pages of Citrix Workspace App and Citrix Virtual Apps and Desktops to ensure you're using supported versions of different components.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- The versions mentioned here are the minimum versions from which the particular feature is supported (or) the minimum version in which New Teams is supported, whichever is higher.
- Citrix Virtual Apps and Desktops 1912 LTSR CU8+ noted in the minimum versions section is not being mentioned in the table below as it will reach it's end of life in December 2024. However, it is still a supported version until then.
- Features that have the minimum Citrix Virtual Apps and Desktops versions as `N/A` just imply that the feature didn't involve any changes from the VDA side.

FEATURE	VDA (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR WINDOWS (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR MAC (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR LINUX (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR CHROMEOS (MINIMUM VERSION)
Audio / Video (p2p and conference)	2203 LTSR (any CU), 2212 CR	2203 LTSR latest CU, 2302 CR	2302	2207	2301
Screensharing	2203 LTSR (any CU), 2212 CR	2203 LTSR latest CU, 2302 CR	2302	2207	2301
i. Screen Indicator Red Border	2203 LTSR (any CU), 2212 CR	2203 LTSR latest CU, 2302 CR	2302	2207	No
ii. Limit capture to Desktop Viewer	2203 LTSR (any CU), 2212 CR	2203 LTSR latest CU, 2302 CR	2302	2207	No
iii. Multimonitor	2203 LTSR (any CU), 2212 CR	2203 LTSR latest CU, 2302 CR	2302	2207	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	VDA (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR WINDOWS (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR MAC (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR LINUX (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR CHROMEOS (MINIMUM VERSION)
DTMF	N/A	2203 LTSR latest CU, 2302 CR	2302	2207	2301
Proxy Server Support	N/A	2203 LTSR latest CU, 2302 CR	2302	2207	2305
App Sharing	2203 LTSR (any CU), 2212 CR	2203 LTSR latest CU, 2302 CR	2302	2209	No
Live Captions	N/A	2203 LTSR latest CU, 2302 CR	2302	2207	2303
Dynamic e911	N/A	2203 LTSR latest CU, 2302 CR	2302	2207	2301
Give Control	N/A	2203 LTSR latest CU, 2302 CR	2302	2207	No
Request Control	N/A	2203 LTSR latest CU, 2302 CR	2302	2207	2303
Multi Window	2203 LTSR (any CU), 2212 CR	2203 LTSR latest CU, 2302 CR	2302	2207	2303
Meeting Transcriptions	2203 LTSR (any CU), 2212 CR	2203 LTSR latest CU, 2302 CR	2302	2207	2303

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	VDA (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR WINDOWS (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR MAC (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR LINUX (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR CHROMEOS (MINIMUM VERSION)
Background blurring	2203 LTSR (any CU), 2212 CR	2203 LTSR latest CU, 2302 CR	2302	2212	2303
Screensharing (with App Protection)	2203 LTSR (any CU), 2212 CR	2402 LTSR, 2309.1 CR	2308	2311	No
Simulcast	2203 LTSR (any CU), 2212 CR	2402 LTSR, 2305 CR	2305	2305	2312
Secondary Ringer	2203 LTSR (any CU), 2212 CR	2402 LTSR, 2307.1 CR	2308	2308	2312
Share System Audio	2203 LTSR (any CU), 2212 CR	2402 LTSR, 2403 CR	2405	2402	No

Troubleshooting and other considerations

For New Teams, see CTX253754 , Troubleshoot Microsoft Teams, For latest updates on anything related to New Teams, see CTX585013.

Known limitations

Limitations on Citrix Workspace app

- HID Support - Answer and end calls aren’t supported. Volume up and down are supported.
- Users can’t take screenshots of Microsoft Teams content while using a snipping tool on the VDA. However, if a snipping tool is used on the client side, the content can be captured.
- Share system audio limitations
    - Audio cannot be shared using this feature when sharing the screen with RAVE and BCR redirected apps or tabs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- This feature is supported only on published desktops

Limitations on the VDA

- New Teams as a published (seamless) application is not supported
  - Fixed in CVAD 2402 LTSR, 2203 LTSR CU5 and above
- When you configure the Citrix Workspace app High DPI setting to Yes, the redirected video window appears out of place. This limitation occurs when the monitor's DPI scaling factor is set to anything above 100%.

Limitations on Citrix Workspace app and the VDA

- You can only control the volume of an optimized call using the volume bar on the client machine – not on the VDA.

For more details on the limitations from Microsoft, see Features not supported in VDI.

New VDI solution for Teams

NOTE:

The New VDI solution for Teams is currently generally available for Windows and Mac endpoints on Citrix®. This solution requires a minimum Microsoft Teams version. See System requirements.

In the New VDI solution for Teams, Microsoft uses the Citrix Virtual Channel SDK to build custom virtual channels. On the endpoint, media is offloaded to the Microsoft media engine (SlimCore) instead of `HdxRtcEngine`. The custom virtual channels carry the communication between Teams on the VDA and the media engine on the endpoint.

NOTE:

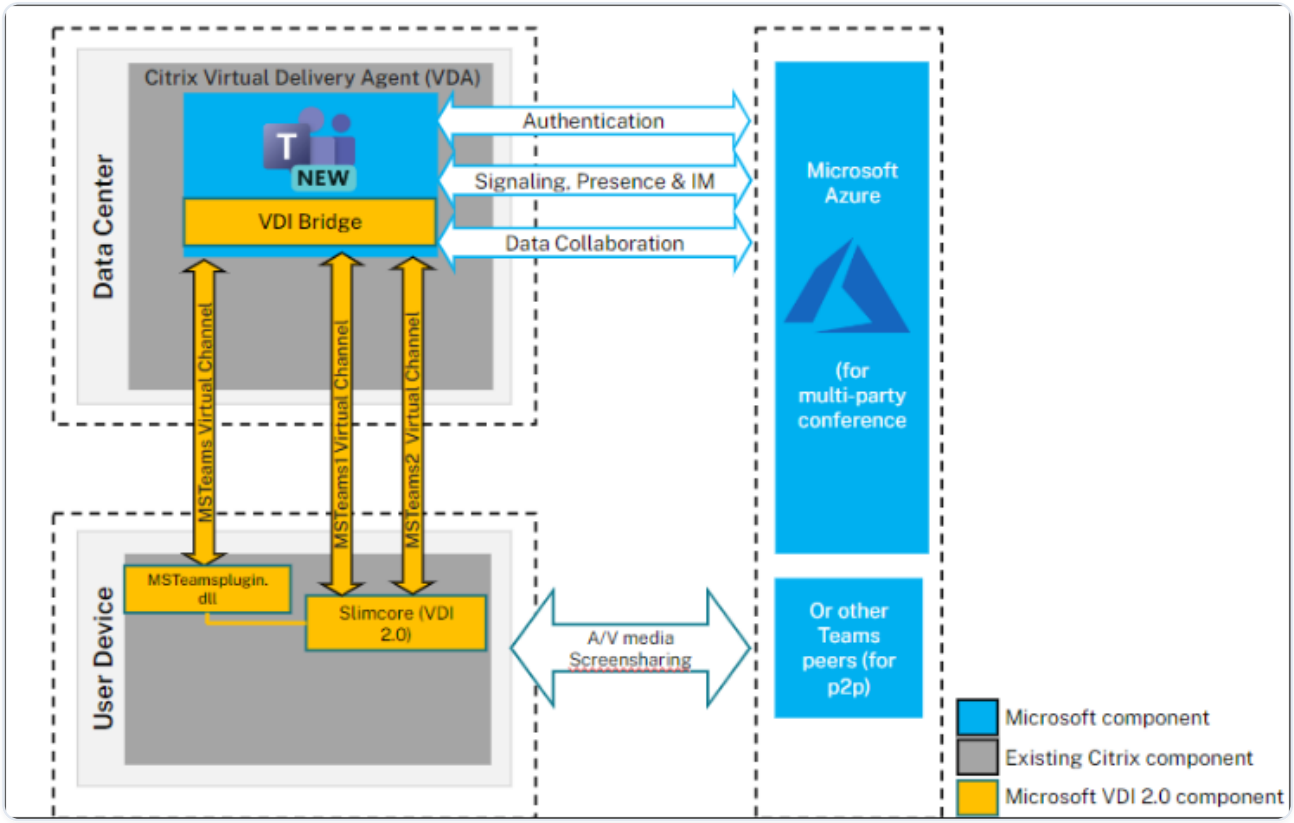
Microsoft has announced the deprecation of WebRTC-based Citrix HDX™ Optimization for Microsoft Teams on Windows endpoints. Two milestones apply:

- October 1, 2026 - End of Support: No longer officially supported by Microsoft or Citrix.
- April 1, 2027 - End of Availability: WebRTC-based optimization stops functioning. Citrix Studio policies for the legacy optimization no longer take effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customers are recommended to migrate to the New VDI solution for Teams. This change affects Windows endpoints only. macOS, Linux, ChromeOS, and HTML5 endpoints are not impacted. For more details, see Microsoft Blog.

This solution is owned and managed by Microsoft. Citrix supports the Citrix components involved: Citrix Workspace™ app, the virtual channel allow list, and the plug-in deployment mechanisms described on this page. For the Microsoft-owned architecture and full details, see New VDI solution for Teams in the Microsoft documentation.



System requirements

This section lists the minimum and recommended versions needed to support the New VDI solution for Teams. On minimum versions, some critical bug fixes or latest features might not be available. Deploy the recommended versions for the best experience.

Virtual Delivery Agent (VDA)

NOTE:

If you are on 2203 LTSR CU2 or below, or 2303 CR or below, see CTX682593 to understand the limitations in those versions and plan your upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MINIMUM VERSIONS	RECOMMENDED VERSIONS
2203 LTSR CU3; 2305 CR	2203 LTSR CU5+; 2402 LTSR and any later CR

Citrix Workspace app for Windows

MINIMUM VERSIONS	RECOMMENDED VERSIONS
2203 LTSR (latest CU); 2302 CR	2402 LTSR; 2405 CR or later

Citrix Workspace app for Mac

MINIMUM VERSIONS	RECOMMENDED VERSIONS
2508.10	2607 or later

Mac endpoints require macOS 14, 15, or 26. macOS 26 requires Citrix Workspace app 2511 or later. On Citrix Workspace app for Mac 2508.10, the plug-in must be installed manually. The option to install the plug-in through Citrix Workspace app, Client App Management, or the Virtual channel plug-in manager is available from Citrix Workspace app for Mac 2603.

For the minimum Microsoft Teams version, endpoint OS requirements, and hardware requirements, see the Microsoft documentation.

Components

- New Teams `vdiBridge`: the server-side virtual channel module, bundled with Teams.
- Custom virtual channel (VC): the custom VC owned by Microsoft Teams.
- Plug-in: the client-side VC dll. Responsible for the media engine download and clean-up.
- Media engine (SlimCore): the operating-system-specific media engine, delivered by Microsoft as an MSIX package.

Deployment

1. Ensure you have the Microsoft Teams version listed in Prerequisites.
2. Configure the **Virtual channel allow list** policy to allow the Microsoft Teams virtual channels. These channels let the Teams client connect to the client-side plug-in. For more information, see Virtual channel security.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The solution needs three custom virtual channels. Use wildcards to allow the `ms-teams.exe` executable and the custom virtual channels:

```
MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
```

NOTE:

- VDA 2603 and later allow these three virtual channels by default. No Studio policy configuration is required on those versions.
- Wildcards for the Virtual channel allow list policy are available in CVAD 2203 LTSR CU2 and later, or Citrix Virtual Apps and Desktops™ 2206 CR and later.
- The VDA machines must be rebooted for the policy to take effect.
- The MSTeams install path changes because it is an MSIX application, so wildcards are required. Allow the exact lines shown above.

3. This solution is controlled by a policy on the Microsoft Teams side, not by a Citrix policy. It is enabled by default. To enable or disable it for specific user groups, see the Microsoft documentation.
4. Deploy the Teams plug-in on your endpoints. See Options to install the Teams plug-in.
5. For media engine staging and registration, and the group policies that can block MSIX installation, see the Microsoft documentation.

Options to install the Teams plug-in

Regardless of the install method, the plug-in is placed in the Citrix Workspace app location on the endpoint:

- Windows (`MsTeamsPluginCitrix.dll`): 64-bit `C:\Program Files (x86)\Citrix\ICA Client`; 32-bit `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

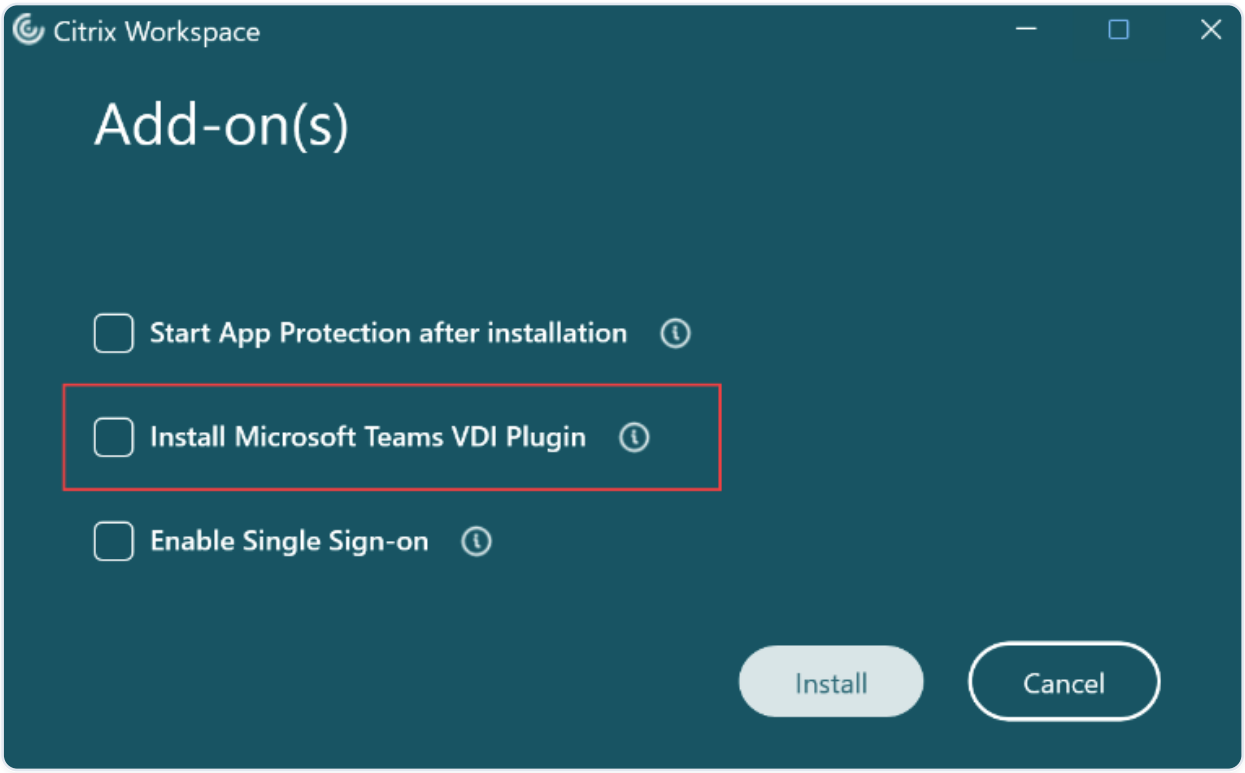
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- On Windows, install Citrix Workspace app in admin mode so virtual channels open correctly. Per-user installation of Citrix Workspace app is not supported.
- The Microsoft Teams VDI plug-in is not supported when Citrix Workspace app is installed from the Microsoft Store.
- Plug-in installation stops if no Citrix Workspace app is found on the endpoint.
- On Windows, the plug-in and Citrix Workspace app must be the same architecture. A 32-bit Citrix Workspace app cannot load a 64-bit plug-in.
- Plug-ins can be upgraded or repaired, but not downgraded, and only while there is no active session.

Option 1: Through Citrix Workspace app installation

- **Windows:** During a fresh install or manual upgrade, select **Install Microsoft Teams VDI Plugin** on the **Add-on(s)** page. From Citrix Workspace app for Windows 2508, this option is selected by default. Clear it to skip installation. Upgrades remember your previous selection.



You can also install from the command line with the `/InstallMSTeamsPlugin` switch. For example, `CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y` installs the plug-in, and `/InstallMSTeamsPlugin=N` prevents it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For a fresh install, the minimum is Citrix Workspace app for Windows 2402 LTSR. For in-place upgrades, the minimum is Citrix Workspace app for Windows 2405 CR. For the latest details, see Install third-party plug-ins.

- **Mac:** The option to install the plug-in during Citrix Workspace app installation is available from Citrix Workspace app for Mac 2603 and requires user action. Citrix Workspace app for Mac 2607 installs the plug-in automatically by default. On Citrix Workspace app for Mac 2508.10, install the plug-in manually. See Option 2: Download the plug-in directly.

Option 2: Download the plug-in directly

- **Windows:** Download the MSI and deploy it with tools like SCCM or Intune on top of any supported Citrix Workspace app version:
  - 32-bit Citrix Workspace app: aka.ms/plugin
  - 64-bit Citrix Workspace app: aka.ms/plugin_x64
  - Arm-based Citrix Workspace app: aka.ms/plugin_arm64
- **Mac:** Download the plug-in from aka.ms/macplugin and deploy it with tools like JAMF.

Option 3: Client App Management (formerly Global App Configuration service)

Client App Management (formerly Global App Configuration service, or GACS) manages app settings for managed and unmanaged endpoints, and can deploy the Teams plug-in across your endpoints. On Mac, this requires Citrix Workspace app for Mac 2603 or later. See Microsoft Teams VDI plug-in management.

Option 4: Virtual channel plug-in manager

The Virtual channel plug-in manager deploys plug-ins across client endpoints for applications that need endpoint components, including the New VDI solution for Teams. It detects the application running on the VDA and prompts the user to install the plug-in on the endpoint. Administrators can use it in BYOD scenarios. On Mac, this requires Citrix Workspace app for Mac 2603 or later. See Virtual channel plugin manager.

Plug-in update scenarios

Citrix handles Teams plug-in updates seamlessly when the plug-in is installed through Options 1, 3, or 4. If the plug-in is installed manually (Option 2), Citrix does not handle updates.

- Ensure Citrix Workspace app auto-update is on for plug-in auto-updates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ensure a minimum of Citrix Workspace app for Windows 2405. Citrix Workspace app for Windows 2508 or later installs the plug-in automatically when Citrix Workspace app auto-updates.
- Citrix does not handle plug-in uninstallation. Uninstall the plug-in separately when needed.

NOTE:

Citrix handles updates to the Teams plug-in, not to the media engine. Microsoft delivers and updates the media engine.

Teams as a Citrix published app

Teams published as a Citrix Virtual Apps application can be optimized with this solution when all the necessary components meet the minimum versions. For the required versions and known limitations, see the Microsoft documentation.

Interoperability and roaming

See Optimization for Microsoft Teams for how the New VDI solution for Teams and Citrix HDX Optimization interoperate and how roaming behaves.

Networking considerations

See Networking considerations in the Microsoft documentation.

Feature support

The feature set and implementation are owned by Microsoft. See the feature list in the Microsoft documentation.

Troubleshooting

The Microsoft Teams client reports the optimization status and, when optimization fails, an error code. These status indicators and error codes are defined by Microsoft. For the full list and end-to-end troubleshooting, see Troubleshooting the New VDI solution for Teams in the Microsoft documentation.

Citrix Monitor provides visibility into the optimization state of this solution. In a session's details, the Session Topology view shows whether the application is optimized and flags any missing components, such as the plug-in manager, the plug-in and its version, the state of the virtual channel, and the virtual channel allow list status. For more information, see Real-time communications optimization visibility.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Some Microsoft error codes point to Citrix-side configuration. Common Citrix checks:

- If the Teams client reports that the custom virtual channels are blocked (Microsoft error 2003), confirm the virtual channel allow list includes MSTEAMS, MSTEAM1, and MSTEAM2.
- If the Teams client reports that no plug-in is detected (Microsoft error 2000), confirm the plug-in is installed and loaded. In Process Explorer, select `wfica32.exe`, show the lower pane, and check the DLL tab for `MsTeamsPluginCitrix.dll`.
- If the Teams client reports an unsupported Citrix Workspace app version (Microsoft error 2004), upgrade to a supported version. See System requirements.

Known limitations

The features and implementation are owned by Microsoft. See Known issues in the Microsoft documentation.

Optimization for Microsoft Teams (Classic)

NOTE:

The new Microsoft Teams 2.1 is now generally available for VDA. This Microsoft Teams version is compatible with Citrix Microsoft Teams Optimization using WebRTC (VDI 1.0).

If you are using Citrix Virtual Apps and Desktops 2402, you don't need to manually configure the `msedgewebview2.exe` registry entry as it's whitelisted by default.
Published apps are now supported with the new Microsoft Teams.
If you are using Citrix Virtual Apps and Desktops 2311 or earlier, a new registry configuration setting is required in the VDA to enable the new Microsoft Teams to access the Citrix virtual channel. To enable Microsoft Teams 2.1 optimization, configure the following registry key in the VDA:
Location: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
Key (REG_Multi_SZ): `ProcessWhitelist`
Value: `msedgewebview2.exe`
For more information, see the Microsoft documentation.
Citrix delivers optimization for desktop-based Microsoft Teams using Citrix Virtual Apps and Desktops™ and Citrix Workspace™ app. By default, we bundle all the necessary components into the Citrix Workspace app and the Virtual Delivery Agent (VDA).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Our optimization for Microsoft Teams includes VDA-side HDX™ services and an API to interface with the Microsoft Teams hosted app to receive commands. These components open a control virtual channel (CTXMTOP) to the Citrix Workspace app-side media engine. The endpoint decodes and provides the multimedia locally, moving the Citrix Workspace app window back into the hosted Microsoft Teams app.

Authentication and signaling occur natively on the Microsoft Teams-hosted app, just like the other Microsoft Teams services (for example chat or collaboration). Audio/video redirection doesn't affect them.

The `CTXMTOP` is a command and control virtual channel. That means that media isn't exchanged between the Citrix Workspace app and the VDA.

Only client-fetch/client-render is available.

This video demo gives you an idea of how Microsoft Teams works in a Citrix virtual environment.



Microsoft Teams installation

Citrix and Microsoft recommend the latest available version of Microsoft Teams and to keep it up to date. Microsoft Teams desktop app versions with release dates that are more than 90 days older than the current version's release date aren't supported. Unsupported Microsoft Teams desktop app versions show a blocking page to users and request to update the app.

For information on the latest available versions, see Update history for Teams App (Desktop and Mac).

We recommend that you follow the Microsoft Teams machine-wide installation guidelines. Also, avoid using the .exe installer that installs Microsoft Teams in `AppData`. Instead, install in `C:\Program Files (x86)\Microsoft\Teams` by using the `ALLUSER=1` flag from the command line.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

This example also uses the `ALLUSERS=1` parameter. When you set this parameter, the Microsoft Teams Machine-Wide Installer appears in **Programs and Features** in the **Control Panel**. Also, in **Apps & features** in Windows Settings for all users of the computer. All users can then uninstall Microsoft Teams if they have administrator credentials.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

It's important to understand the difference between `ALLUSERS=1` and `ALLUSER=1`. You can use the `ALLUSERS=1` parameter in non-VDI and VDI environments. Use the `ALLUSER=1` parameter only in VDI environments to specify a per-machine installation.

In `ALLUSER=1` mode, the Microsoft Teams application doesn't auto-update whenever there's a new version. We recommend this mode for non-persistent environments, such as hosted shared apps or desktops out of a Windows Server or Windows 10 random/pooled catalogs. For more information, see Install Microsoft Teams using MSI (VDI Installation section).

Suppose you have Windows 10 dedicated persistent VDI environments. You want the Microsoft Teams application to auto-update and prefer Microsoft Teams to install per-user under `Appdata/Local`. In this case, use the `.exe` installer or the MSI without `ALLUSER=1`.

NOTE:

We recommend installing the VDA before installing Microsoft Teams in the golden image. This installation order is needed for the `ALLUSER=1` flag to take effect. If you installed Microsoft Teams in the virtual machine before installing the VDA, uninstall and reinstall Microsoft Teams.

For Remote PC Access

We recommend that you install Microsoft Teams version 1.4.00.22472 or later after installing the VDA. Otherwise, you need to sign out and sign in again for Microsoft Teams to detect the VDA as expected. Version 1.4.00.22472 and later includes augmented logic run at Microsoft Teams launch time and sign in time for VDA detection. These versions also include active session type identification (HDX, RDP or locally connected to the client machine). If you're locally connected, previous versions of Microsoft Teams might fail to detect and disable certain features or UI elements. For example, Breakout Rooms, pop out windows for meetings and chat, or meeting reactions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

When you roam from a local session to an HDX session and if Microsoft Teams is kept open and running on the background, you must exit and relaunch Microsoft Teams to optimize with HDX correctly. Conversely, if you use Microsoft Teams remotely via an optimized HDX session, disconnect the HDX session and reconnect to the same Windows session locally at the device. When working from the office, you must relaunch Microsoft Teams so it can correctly detect the Remote PC state (HDX or local). Because Microsoft Teams can only assess VDI mode at app launch time, and not while it is already running on the background. Without a restart, Microsoft Teams might fail to load features like pop out Windows, Breakout Rooms, or meeting reactions.

For App Layering

If using Citrix App Layering to manage VDA and Microsoft Teams installations in different layers, you must create a new registry key on Windows VDAs before installing Microsoft Teams with the `ALLUSER=1` flag from the command line. For more information, see the *Optimization for Microsoft Teams with Citrix App Layering* section under Multimedia.

Profile Management recommendations

We recommend using the machine-wide installer for Windows Server and Pooled VDI Windows 10 environments.

When the **ALLUSER=1** flag is passed to the MSI from the command line (the machine-wide installer), the Microsoft Teams app installs under `C:\Program Files (x86)` (~300 MB). The app uses `AppData\Local\Microsoft\TeamsMeetingAddin` for logs and `AppData\Roaming\Microsoft\Teams` (~600–700 MB) for user specific configurations, caching of elements in the user interface, and so forth.

IMPORTANT:

If you don't pass the **ALLUSER=1** flag, the MSI places the Teams.exe installer and `setup.json` under `C:\Program Files (x86)\Teams Installer`. A registry key (TeamsMachineInstaller) is added under: `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`

A subsequent user logon triggers the final installation in **AppData** instead.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Machine-wide installer

The following is an example of folders, desktop shortcuts, and registries created by installing Microsoft Teams machine-wide installer on a Windows Server 2016 64-bit VM:

Folder:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Desktop Shortcut:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

Registry:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Name: `Teams`
- Type: `REG_SZ`
- Value: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

NOTE:

The registry location varies based on the underlying Operating Systems and bitness.

Recommendations

- We recommend disabling auto-start by deleting the Microsoft Teams registry keys. Doing so prevents many logons that occur at the same time (for example, at the beginning of your work day) from spiking up the VM's CPU.
- If the virtual desktop does not have a GPU/vGPU, we recommend setting **Disable GPU hardware acceleration** in the Microsoft Teams **Settings** to improve performance. This setting (`"disableGpu":true`) is stored in `%Appdata%\Microsoft\Teams` in `desktop-config.json`. You can use a logon script to edit that file and set the value to **true**.
- If using Citrix Workspace Environment Management™ (WEM), enable **CPU Spikes Protection** to manage processor consumption for Microsoft Teams.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Per-user installer

When using the `.exe` installer, the installation process differs. All the files are placed in AppData.

Folder:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Desktop shortcut:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

Registry:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Best Practices

The best practice recommendations are based on the use-case scenarios. Using Microsoft Teams with a non-persistent setup requires a profile caching manager for efficient Microsoft Teams runtime data synchronization. With a profile caching manager, the appropriate user-specific information is cached during the user session. For example, the user-specific information includes, user data, profile, and settings. Synchronize the data in these two folders:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Microsoft Teams cached content exclusion list for non-persistent setup

Exclude the files and directories from the Microsoft Teams caching folder as described in the Microsoft documentation. This action helps you to reduce the user caching size to further optimize your non-persistent setup.

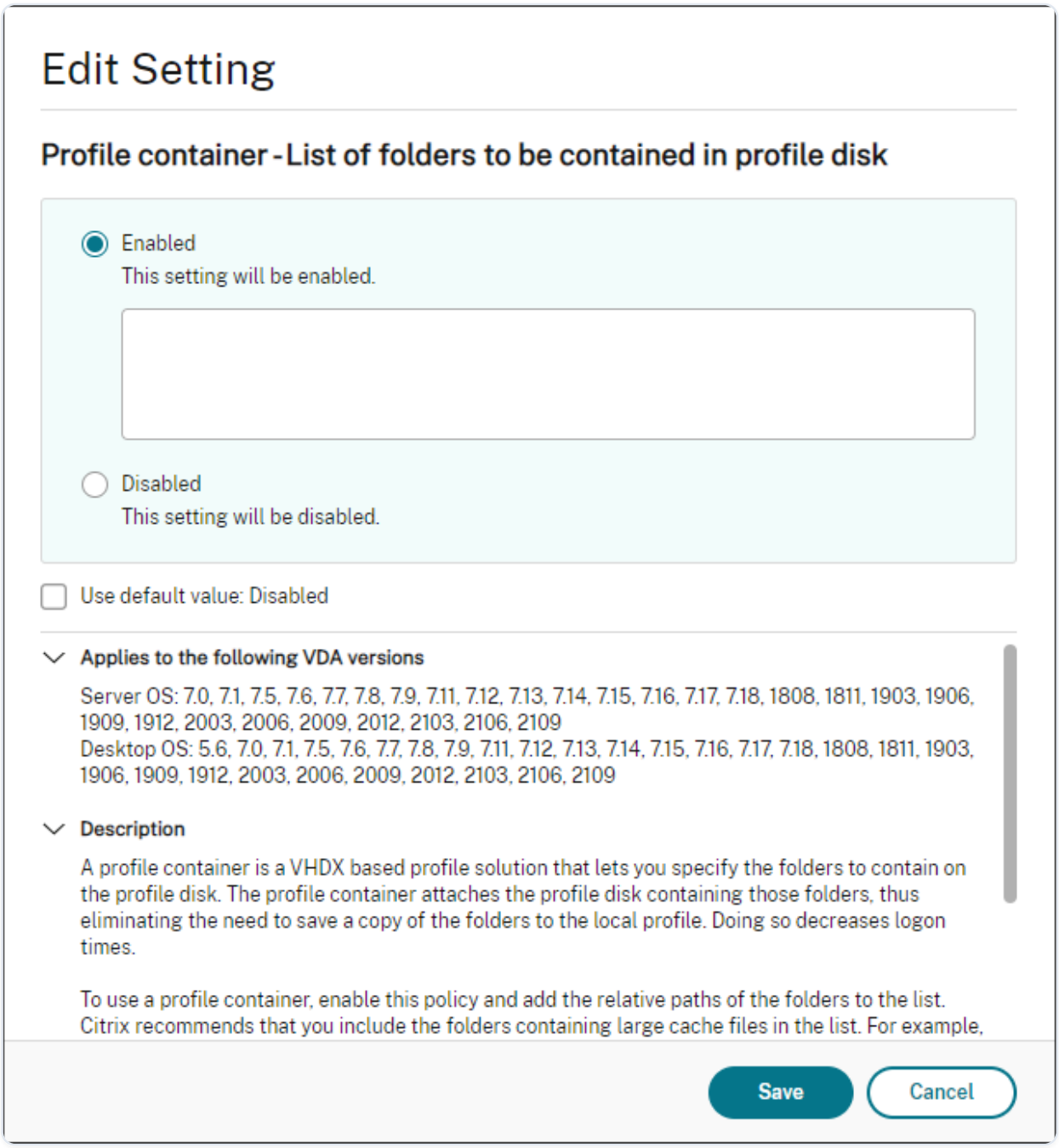
Use case: single-session scenario

In this scenario, the end user uses Microsoft Teams in one location at a time. They don't need to run Microsoft Teams in two Windows sessions at the same time. In a common virtual desktop deployment, each user is assigned to one desktop, and Microsoft Teams is deployed in the virtual

© 1997–2026 Citrix Systems, Inc. All rights reserved.

desktop as one application. We recommend enabling the Citrix Profile container and redirecting the per-user directories listed in Per-user installer into the container.

1. Deploy the Microsoft Teams machine-wide installer (**ALLUSER=1**) in the golden image.
2. Enable Citrix Profile Management and set up the user profile store with the proper permissions.
3. Enable the following Profile Management policy setting: **File system > Synchronization > Profile container – List of folders to be contained in profile disk**.



List all the per-user directories into this configuration. You can also configure these settings using the Citrix Workspace Environment Management (WEM) service.

4. Apply the settings to the correct delivery group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Log in to validate the deployment.

System requirements

Minimum recommended version - Delivery Controller (DDCs) 1906.2

If you're using an earlier version, see Enable optimization of Microsoft Teams:

Supported operating systems:

- Windows Server 2022, 2019, 2016, 2012R2 Standard and data center Editions, and with the Server Core option

Minimum version - Virtual Delivery Agents (VDAs) 1906.2

Supported operating systems:

- Windows 11.
- Windows 10 64-bit, versions 1607 and later. VM hosted apps are supported in Citrix Workspace app for Windows 2109.1 and later.
- Windows Server 2022, 2019, 2016, and 2012 R2 (Standard and data center Editions).

Requirements:

- BCR_x64.msi - the MSI that includes the Microsoft Teams optimization code and starts automatically from the GUI. If you're using the command line interface for the VDA installation, don't exclude it.

Recommended version – Citrix Workspace app for Windows latest CR and Minimum version - Citrix Workspace app 1907 for Windows

- Windows 11.
- Windows 10 (32-bit and 64-bit editions, including Embedded editions) (Support for Windows 7 stopped at Version 2006) (Support for Windows 8.1 stopped at version 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) and 2019 LTSC (v1809).
- Processor (CPU) architectures supported: x86 and x64 (ARM isn't supported).
- Endpoint requirement: Approximately 2.2–2.4 GHz dual core CPU that can support 720p HD resolution during a peer-to-peer video conference call.
- Dual or quad-core CPUs with lower base speeds (~1.5 GHz) equipped with Intel Turbo Boost or AMD Turbo Core that can boost up to at least 2.4 GHz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HP Thin Clients verified: t630/t640, t730/t740, mt44/mt45.
- Dell Thin Clients verified: 5070, 5470 Mobile TC and AIO.
- 10ZiG Thin Clients verified: 4510 and 5810q.
- For a complete list of verified endpoints, see Thin Clients.
- Citrix Workspace app requires at least 600 MB free disk space and 1 GB RAM.
- Microsoft .NET Framework minimum requirement is version 4.8. Citrix Workspace app automatically downloads and installs .NET Framework if it's not present in the system.

Administrators can enable/disable Microsoft Teams starting in optimized mode by changing the Teams Optimization policy. Users starting in optimized mode in Citrix Workspace app can't disable Microsoft Teams.

Minimum version - Citrix Workspace app 2006 for Linux

Software:

- `GStreamer` 1.0 or later or Cairo 2
- libc++-9.0 or later
- `libgdk` 3.22 or later
- OpenSSL 1.1.1d
- x64 Linux distribution

Hardware:

- Minimum 1.8 GHz dual-core CPU that can support 720p HD resolution during a peer-to-peer video conference call
- Dual or quad-core CPU with a base speed of 1.8 GHz and a high Intel Turbo Boost speed of at least 2.9 GHz

For a complete list of verified endpoints, see Thin Clients.

For more information, see Prerequisites to install Citrix Workspace app.

You can disable Microsoft Teams optimization updating the value of the **VDWEBRTC** field to Off in the `/opt/Citrix/ICAClient/config/module.ini` file. The default is VDWEBRTC=On. After the update is complete, restart the Session. (Root permission is required).

Minimum version - Citrix Workspace app 2012 for Mac

Supported operating systems:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 and later.
- macOS Monterey.

Features supported:

- Audio
- Video
- Screen sharing optimization (incoming and outgoing)

NOTE:

Citrix Viewer app requires access to macOS Security and Privacy preferences for screen sharing to work. Users configure this preference in **Apple menu > System preferences > Security & Privacy > Privacy tab > Screen recording** and select **Citrix Viewer**.

Microsoft Teams optimization works by default with Citrix Workspace app 2012 and later and macOS 10.15.

If you want to disable Microsoft Teams optimization, run this command in a terminal and restart the Citrix Workspace app:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

Minimum version - Latest version of Citrix Workspace app for Chrome OS running on the latest version of Chrome OS

Hardware:

- Processors that perform at par or better than Intel i3, quad core 2.4 GHz.

Features supported:

- Audio
- Video
- Screen sharing optimization (incoming and outgoing) - disabled by default. See these settings for instructions on how to turn it on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Single Server Scalability

This section provides recommendations and guidance to estimate how many users or virtual machines (VMs) can be supported on a single physical host. This is commonly referred to as Citrix Virtual Apps and Desktops Single Server Scalability (SSS). In the context of Citrix Virtual Apps (CVA) or session virtualization, it is also commonly known as user density. The idea is to find out how many users or VMs can be ran on a single piece of hardware running a major hypervisor.

NOTE:

This section includes guidance to estimate SSS. Note that the guidance is high level and might not necessarily be specific to your unique situation or environment. The only way to truly understand Citrix Virtual Apps and Desktops SSS is to use a scalability or load testing tool such as Login VSI. Citrix recommends using this guidance and these simple rules to quickly estimate SSS only. However, Citrix recommends using Login VSI or the load testing tool of your choice to validate results, especially before purchasing hardware or making any financial decisions.

Hardware (system under test)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (max Turbo 3.70 GHz), 12 cores per socket, dual socket with Hyperthreading enabled
- 382 GB of RAM
- Local SSD RAID 0 storage (11 disk) 6 TB

Software

A single virtual machine (40 logical processors) with Windows 2019 (TSVDA) running Citrix Virtual Apps and Desktops 2106 VMware ESXi 6.7

Terminology

- Knowledge worker workload: Includes Acrobat Reader, Freemind/Java, Photo viewer, Edge, and MS Office apps such as Excel, Outlook, PowerPoint, and Word.
- Baseline: Server Scalability tests run with knowledge worker workload (without Microsoft Teams).
- Microsoft Teams Workload: Knowledge worker typical workload + Microsoft Teams.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How Microsoft Teams is stress-tested

- Microsoft Teams is optimized with HDX. Hence, all the multimedia processing is offloaded to the endpoint or client and is not part of the measurement.
- All Microsoft Teams processes stopped or killed, before workload starts.
- Open Microsoft Teams (Cold start).
- Measure the time taken by Microsoft Teams to load and grab the focus of Microsoft Teams primary window.
- Switch to chat window using keyboard shortcuts.
- Switch to calendar window using keyboard shortcuts.
- Send the chat message to a specific user using keyboard shortcuts.
- Switch to Microsoft Teams window using keyboard shortcuts.

Results

- 40% scalability impact with Microsoft Teams Workload (81 users), when compared to Baseline (137 users).
- Increasing the server capacity by ~40% (in CPU) restores the number of users as with Baseline workload.
- 20% extra memory required with Microsoft Teams Workload, when compared to Baseline.
- Increase per user storage size by 512-1024 MB.
- ~50% increase in IOPS write, ~100% increase in IOPS reads. Microsoft Teams can have a significant impact in environment with slower storage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature matrix and version support

FEATURE	MICROSOFT TEAMS (MINIMUM VERSION)	VDA (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR WINDOWS CR (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR MAC (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR LINUX (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR CHROME OS
Audio/ Video (P2P and conference)	current version minus 90 days	1906	1907	2009	2004	2105.5
Screensharing	Current version minus 90 days	1906	1907	2012	2006	2105.5
i. Screen Indicator Red border	Current version minus 90 days	1906	2002	2012	2006	No
ii. Limit capture to Desktop Viewer	Current version minus 90 days	1906	2009.5	2012	2006	No
iii. Multimonitor	Current version minus 90 days	1912 CU6+	2106 (1)	2106	2106	No
DTMF	Current version minus 90 days	N/A	2102	2101	2101	2111.1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	MICROSOFT TEAMS (MINIMUM VERSION)	VDA (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR WINDOWS CR (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR MAC (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR LINUX (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR CHROME OS
Proxy Server support	Current version minus 90 days	N/A	2012 (2)	2104 (3)	2101 (3)	2305
App Sharing	Current version minus 90 days	2109	2109.1	2203.1	2209	No
Live Captions	Current version minus 90 days	N/A (4)	2109.1	2109	2109	2303
Dynamic e911	Current version minus 90 days	N/A	2112.1	2112	2112	2112
Give Control	Current version minus 90 days	N/A	2112.1	2203.1	No	No
Request Control	Current version minus 90 days	N/A	2112.1	2203.1	2203	2303
MultiWindow	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	MICROSOFT TEAMS (MINIMUM VERSION)	VDA (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR WINDOWS CR (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR MAC (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR LINUX (MINIMUM VERSION)	CITRIX WORKSPACE APP FOR CHROME OS
Meeting Transcriptions	Current version minus 90 days	2112.1, 1912 CU6+	2112	2203.1	2203	2303
Background Blurring	Current version minus 90 days	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewer in full screen mode only. SHIFT+F2 not supported.
2. Negotiate/Kerberos, NTLM, Basic, and Digest. `Pac` files are also supported.
3. Anonymous only.
4. If VDA is 2112 or higher, Live Captions will only work if Citrix Workspace app version is 2203.1 for MAC and 2203 Linux or 2112 for Windows. This is because Live Captions behave differently if Microsoft Teams is in Single Window UI mode or MultiWindow mode.
5. MultiWindow was introduced in 2112 VDA but was back-ported to the VDA 1912 LTSR CU6 release.

NOTE:

All features listed in **Citrix Workspace app for Windows 1912 CU6 (or later)** are applicable to Citrix Workspace app for Windows 2203.1 LTSR CU1.

Enable optimization of Microsoft Teams

To enable optimization for Microsoft Teams, use the Studio policy described in the Microsoft Teams redirection policy. This policy is **ON** by default. In addition to this policy being enabled, HDX checks to verify that the version of the Citrix Workspace app is at least the minimum required version. If

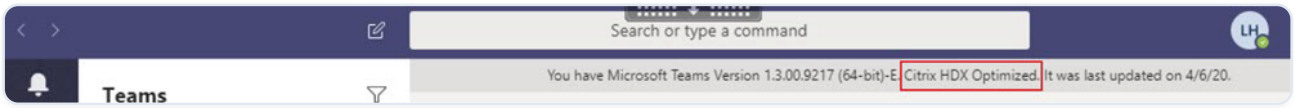
© 1997–2026 Citrix Systems, Inc. All rights reserved.

you enabled the policy and the Citrix Workspace app version is supported, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** is set to **1** automatically on the VDA. Microsoft Teams reads the key to load in VDI mode.

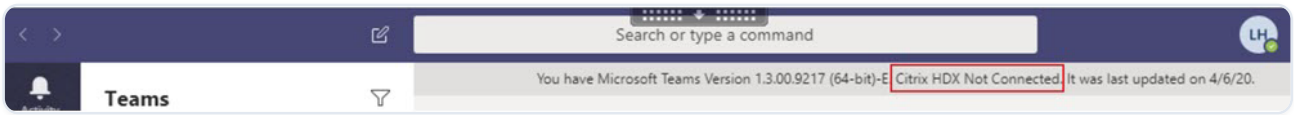
NOTE:

If you're using version 1906.2 or later VDAs or with older controller versions (for example, version 7.15) that don't have the policy available in Studio, your VDA can still be optimized. HDX optimization for Microsoft Teams is enabled by default in the VDA.

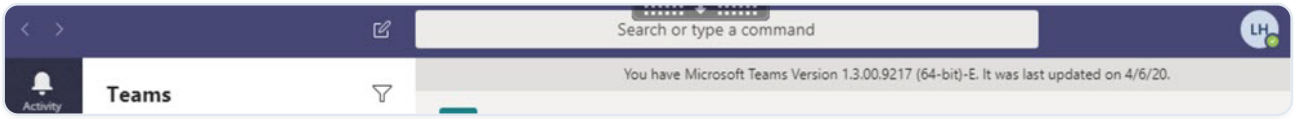
If you click **About > Version**, the **Citrix HDX Optimized** legend displays:



If you see **Citrix HDX Not Connected**, the Citrix API is loaded in Microsoft Teams. Loading the API is the first step toward redirection. But there's an error in later parts of the stack. The error is most likely in the VDA services or the Citrix Workspace app.



If you don't see any legend, Microsoft Teams failed to load the Citrix API. Exit Microsoft Teams by right-clicking the notification area icon and restarting. Make sure that the Studio policy isn't set to **Prohibited** and that the Citrix Workspace app version is supported.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT: SESSION RECONNECTS

- You might require to relaunch Microsoft Teams to get an HDX optimized session when your connectivity changes. For example, if you are roaming from an unsupported endpoint (Workspace app for iOS, Android, or old versions of Windows/Linux/Mac) to a supported one (Workspace app for Windows/Linux/Mac/ChromeOS/HTML5), or the opposite way.
- A Microsoft Teams relaunch is also required if you have installed the app using the Microsoft Teams .exe installer in the VDA. The .exe installer is recommended for persistent VDI deployments. In such cases, Microsoft Teams can auto-update while the HDX session is in the disconnected state. So, users reconnecting to an HDX session finds that the Microsoft Teams is not running optimized.
- When you roam from a local session to an HDX session, you must relaunch Microsoft Teams to optimize with HDX. This action is required in a Remote PC Access scenario.

Network requirements

Microsoft Teams relies on Media Processor servers in Microsoft 365 for meetings or multiparty calls. Also, Microsoft Teams relies on Microsoft 365 Transport Relays for these scenarios:

- Two peers in a point-to-point call do not have direct connectivity
- A participant does not have direct connectivity to the media processor.

So the network health between the peer and the Microsoft 365 cloud determines the performance of the call. For detailed guidelines around network planning, see Microsoft 365 network connectivity principles.

We recommend evaluating your environment to identify any risks and requirements that can influence your overall cloud voice and video deployment. Use the Skype for Business Network Assessment Tool to test if your network is ready for Microsoft Teams. For support information, see Support.

Summary of key network recommendations for Real Time Protocol (RTP) traffic

- Connect to the Microsoft 365 network as directly as possible from the branch office.
- Plan for and provide sufficient bandwidth at the branch office.
- Check each branch office for network connectivity and quality.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you must use any of the following at the branch office, make sure that RTP/UDP traffic (handled by HdxRtcEngine.exe in Citrix Workspace app) is.
  - Bypass proxy servers
  - Network SSL intercept
  - Deep packet inspection devices
  - VPN hairpins (use split tunneling if possible)

IMPORTANT: VPN SPLIT TUNNEL CONFIGURATION

HdxRtcEngine.exe traffic has to be diverted from the VPN tunnel and allowed to use the user's local Internet connection to connect directly to the service. The manner in which this is accomplished will vary depending on the VPN product and machine platform used but most VPN solutions will allow some simple configuration of policy to apply this logic. For more information on VPN platform-specific split tunnel guidance, see this Microsoft article.

The WebRTC media engine in the Workspace app (HdxRtcEngine.exe) uses the Secure Real-time Transport Protocol (SRTP) for multimedia streams that are offloaded to the client. SRTP provides confidentiality and authentication to RTP. For this feature, symmetric keys (negotiated with DTLS) are used to encrypt media and control messages using the AES encryption cipher.

The following metrics are recommended for a positive user experience:

METRIC	ENDPOINT TO MICROSOFT 365
Latency (one way)	< 50 msec
Latency (RTT)	< 100 msec
Packet Loss	<1% during any 15s interval
Packet inter-arrival jitter	<30ms during any 15s interval

For more information, see Prepare your organization's network for Microsoft Teams.

For bandwidth requirements, optimization for Microsoft Teams can use a wide variety of codecs for audio (OPUS/G.722/PCM G711) and video (H264).

The peers negotiate these codecs during the call establishment process using the Session Description Protocol (SDP) Offer/Answer. Citrix minimum recommendations per user are:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE	BANDWIDTH	CODEC
Audio (each way)	~ 90 kbps	G.722
Audio (each way)	~ 60 kbps	Opus*
Video (each way)	~ 700 kbps	H264 360p @ 30 fps 16:9
Screen sharing	~ 300 kbps	H264 1080p @ 15 fps

Opus and H264 are the preferred codecs for peer-to-peer and conference calls.

IMPORTANT:

About performance, encoding is more expensive than decoding for CPU use at the client machine. You can hardcode the maximum encoding resolution in the Citrix Workspace app for Linux and Windows. See Encoder performance estimator and Optimization for Microsoft Teams.

Proxy servers

Depending on the location of the proxy, consider the following:

- Proxy configuration on the VDA:

  If you configure an explicit proxy server in the VDA and route connections to localhost through a proxy, redirection fails. To configure the proxy correctly, you must select the **Bypass proxy servers for local address** setting in **Internet Options > Connections > LAN Settings > Proxy Servers** and bypass `127.0.0.1:9002`.

  If you use a PAC file, your VDA proxy configuration script from the PAC file must return **DIRECT** for `wss://127.0.0.1:9002`. If not, optimization fails. To make sure that the script returns **DIRECT**, use `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Proxy configuration on Citrix Workspace app:

  If the branch office is configured to access the internet through a proxy, these versions support proxy servers:

  - Citrix Workspace app for Windows version 2012 (Negotiate/Kerberos, NTLM, Basic, and Digest. `Pac` files are also supported)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Workspace app for Windows version 1912 CU5 (Negotiate/Kerberos, NTLM, Basic, and Digest. `Pac` files are also supported)
- Citrix Workspace app for Linux version 2101 (anonymous authentication)
- Citrix Workspace app for Mac version 2104 (anonymous authentication)

Client devices with earlier versions of Citrix Workspace app can't read proxy configurations. These devices send traffic directly to Microsoft 365 TURN servers.

IMPORTANT:

- Verify that the client device can connect to the DNS server to do DNS resolutions. A client device must be able to resolve the following Microsoft Teams Relay server's FQDNs:
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

If DNS requests are unsuccessful, P2P calls with outside users and conference calls media establishment fails.

- The location of the conference server is selected based on the first participant's virtual desktop location (and not the client).

Call establishment and media flow paths

When possible, the HDX WebRTC media engine in the Citrix Workspace app (HdxRtcEngine.exe) tries to establish a direct network Secure Real-time Transport Protocol (SRTP) connection over User Datagram Protocol (UDP) in a peer-to-peer call. If the UDP high ports are blocked, the media engine falls back to TCP/TLS 443.

The HDX media engine supports ICE, Session Traversal Utilities for NAT (STUN), and Traversal Using Relays around NAT (TURN) for candidate discovery and establishing connection. This support means that the endpoint must be able to perform DNS resolutions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Consider a scenario where there is no direct path between the two peers or between a peer and a conference server and you are joining a multi-party call or meeting. The HdxRtcEngine.exe uses a Microsoft Teams transport relay server in Microsoft 365 to reach the other peer or the media processor, where meetings are hosted. Your client machine must have access to three Microsoft 365 subnet IP address ranges and four UDP ports (or TCP/TLS 443 as fallback if UDP is blocked). For more information, see the Architecture diagram in the Call setup and Office 365 URLs and IP address ranges ID 11.

ID	CATEGORY	ADDRESSES	DESTINATION PORTS
11	Optimize required	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (fallback)

These ranges include both Transport Relays and media processors, front-ended by an Azure Load Balancer. The Microsoft Teams Transport Relays provide STUN and TURN functionality, but they aren't ICE endpoints. Also, the Microsoft Teams Transport Relays don't terminate media, TLS, or do any transcoding. They can bridge TCP (if HdxRtcEngine.exe uses TCP) to UDP when they forward traffic to other peers or media processors.

Workspace app WebRTC media engine contacts the closest Microsoft Teams Transport Relay in the Microsoft 365 cloud. The media engine uses anycast IP and port 3478–3481 UDP (different UDP ports per workload, though multiplexing can happen) or 443 TCP/TLS for fallbacks. Call quality depends on the underlying network protocol. Because UDP is always recommended over TCP, we advise you to design your networks to accommodate UDP traffic in the branch office.

If Microsoft Teams loaded in optimized mode and HdxRtcEngine.exe is running on the endpoint, ICE failures might cause a call setup failure or one-way-only audio/video. When a call can't be completed or the media streams aren't full duplex, check the **Wireshark trace** on the endpoint first. For more information about the ICE candidate gathering process, see "Collecting logs" in the Support section.

NOTE:

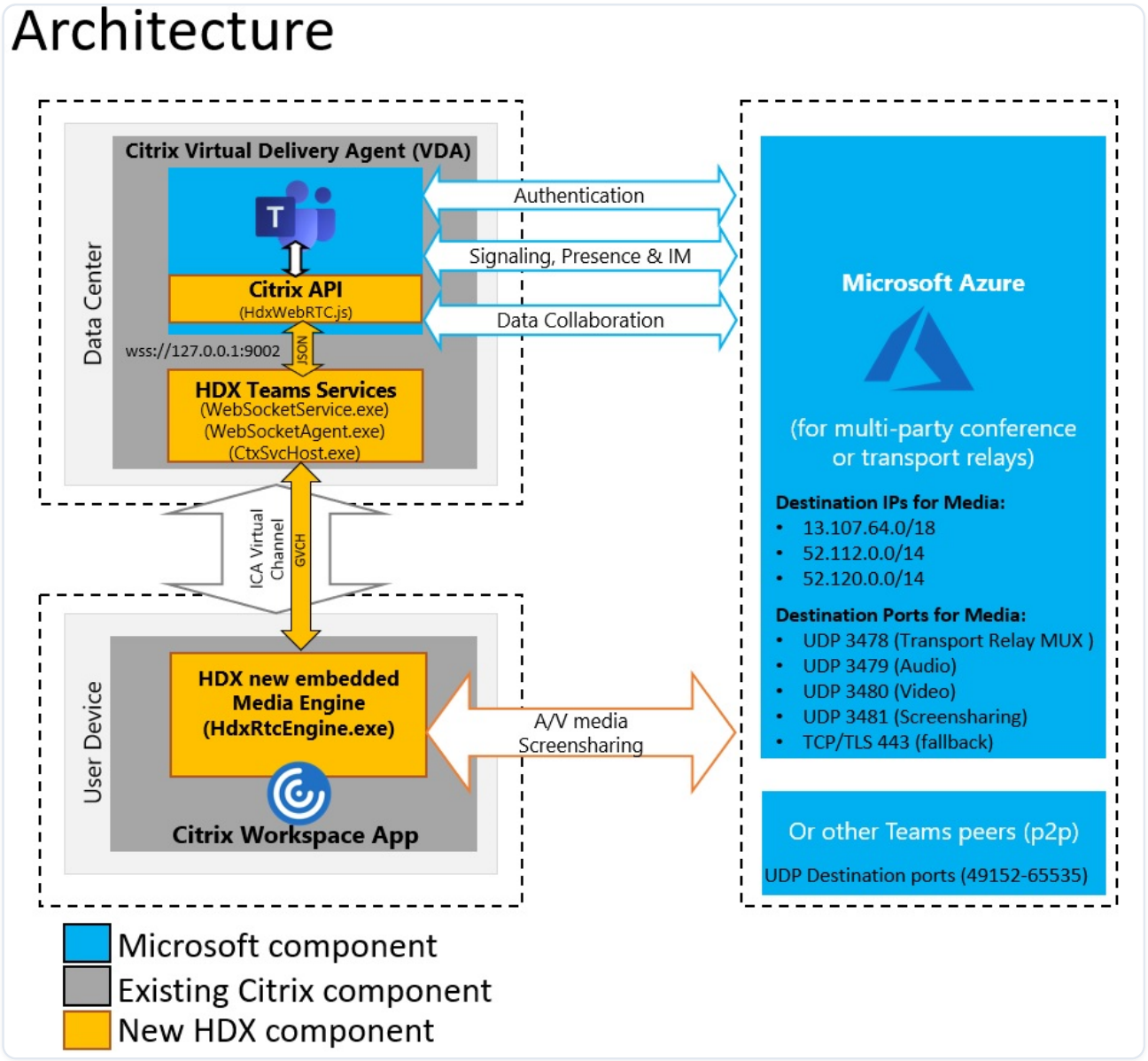
If the endpoints don't have internet access, the users might still be able to make a peer-to-peer call if they are both on the same LAN. Meetings fail. In this case, there's a 30-second timeout before the call setup begins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Call setup

Use this architecture diagram as a visual reference for the call flow sequence. The corresponding steps are indicated in the diagram.

Architecture



1. Start Microsoft Teams.
2. Microsoft Teams authenticates to O365. Tenant policies are pushed down to the Microsoft Teams client, and relevant TURN and signaling channel information is relayed to the app.
3. Microsoft Teams detects that it's running in a VDA and makes API calls to the Citrix JavaScript API.
4. Citrix JavaScript in Microsoft Teams opens a secure WebSocket connection to WebSocketService.exe running on the VDA, which spawns WebSocketAgent.exe inside the user session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. WebSocketAgent.exe instantiates a generic virtual channel by calling into the Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe).
6. Citrix Workspace app's wfica32.exe (HDX engine) spawns a new process called HdxRtcEngine.exe, which is the new WebRTC engine used for Microsoft Teams optimization.
7. Citrix media engine and Teams.exe have a 2-way virtual channel path and can start processing multimedia requests.

   -----User calls------

8. **Peer A** clicks the **call** button. Teams.exe communicates with the Microsoft Teams services in Microsoft 365, establishing an end-to-end signaling path with **Peer B**. Microsoft Teams asks HdxRtcEngine for a series of supported call parameters (codecs, resolutions, and so forth, which is known as a Session Description Protocol (SDP) offer). These call parameters are then relayed using the signaling path to the Microsoft Teams services in Microsoft 365 and from there to the other peer.
9. The SDP offer/answer (single-pass negotiation) takes place through the signaling channel, and the ICE connectivity checks (NAT and Firewall traversal using STUN bind requests) complete. Then, Secure Real-time Transport Protocol (SRTP) media flows directly between HdxRtcEngine and the other peer (or Microsoft 365 conference servers if it's a meeting).

Microsoft Phone System

Phone System is Microsoft's technology that enables call control and PBX in the Microsoft 365 cloud with Microsoft Teams. Optimization for Microsoft Teams supports Phone System, using Microsoft 365 Calling Plans or Direct Routing. With Direct Routing, you connect your own supported session border controller to the Microsoft Phone System directly without any additional on-premises software. Call queues, transfer, forward, hold, mute, and resume a call are supported.

DTMF

The dual-tone multi-frequency (DTMF) feature is supported with these versions of Citrix Workspace app (and later):

- Citrix Workspace app for Windows version 2102
- Citrix Workspace app for Windows LTSR 1912 CU5 (Windows 10 OS only)
- Citrix Workspace app for Linux version 2101
- Citrix Workspace app for Mac version 2101
- Citrix Workspace app for Chrome OS version 2111.1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for dynamic e911

Starting with version 2112, Citrix Workspace app supports dynamic emergency calling. When used in Microsoft Calling Plans, Operator Connect, and Direct Routing, it allows you to do the following:

- Configure and route emergency calls.
- Notify security personnel.

The notification is provided based on the current location of the Citrix Workspace app that runs on the endpoint, instead of the Microsoft Teams client that runs on the VDA.

Ray Baum's law requires the 911 caller's dispatchable location to be transmitted to the appropriate Public Safety Answering Point (PSAP). Microsoft Teams Optimization with HDX is compliant with Ray Baum's law when used with the following versions of Citrix Workspace app:

- Citrix Workspace app for Windows version 2112.1 and later
- Citrix Workspace app for Linux version 2112 and later
- Citrix Workspace app for Mac version 2112 and later
- Citrix Workspace app for Chrome OS version 2112 and later

To enable dynamic emergency calling, the administrator must use the Microsoft Teams Admin Center and configure the following to create a network or emergency location map:

- Network settings
- Location Information Service (LIS)

For more information on Dynamic emergency calling, see Microsoft's documentation.

The dispatchable location information that Citrix Workspace app relays to Microsoft Teams is:

- Chassis ID / Port ID using Link Layer Discovery Protocol (LLDP) for Ethernet/Switch connections. Ethernet/Switch (LLDP) is supported on:
  - Windows versions 8.1 and 10
  - macOS, which requires LLDP enablement software. To download the LLDP enablement software, go to `www.microsoft.com` and search for LLDP enablement software.
  - Linux, which requires the LLDP library to be included in the operating system(OS) distribution of the Thin Client.
- WLAN BBSID and {IPv4-IPv6; Subnet; MAC Address} of the endpoint where Citrix Workspace app is installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

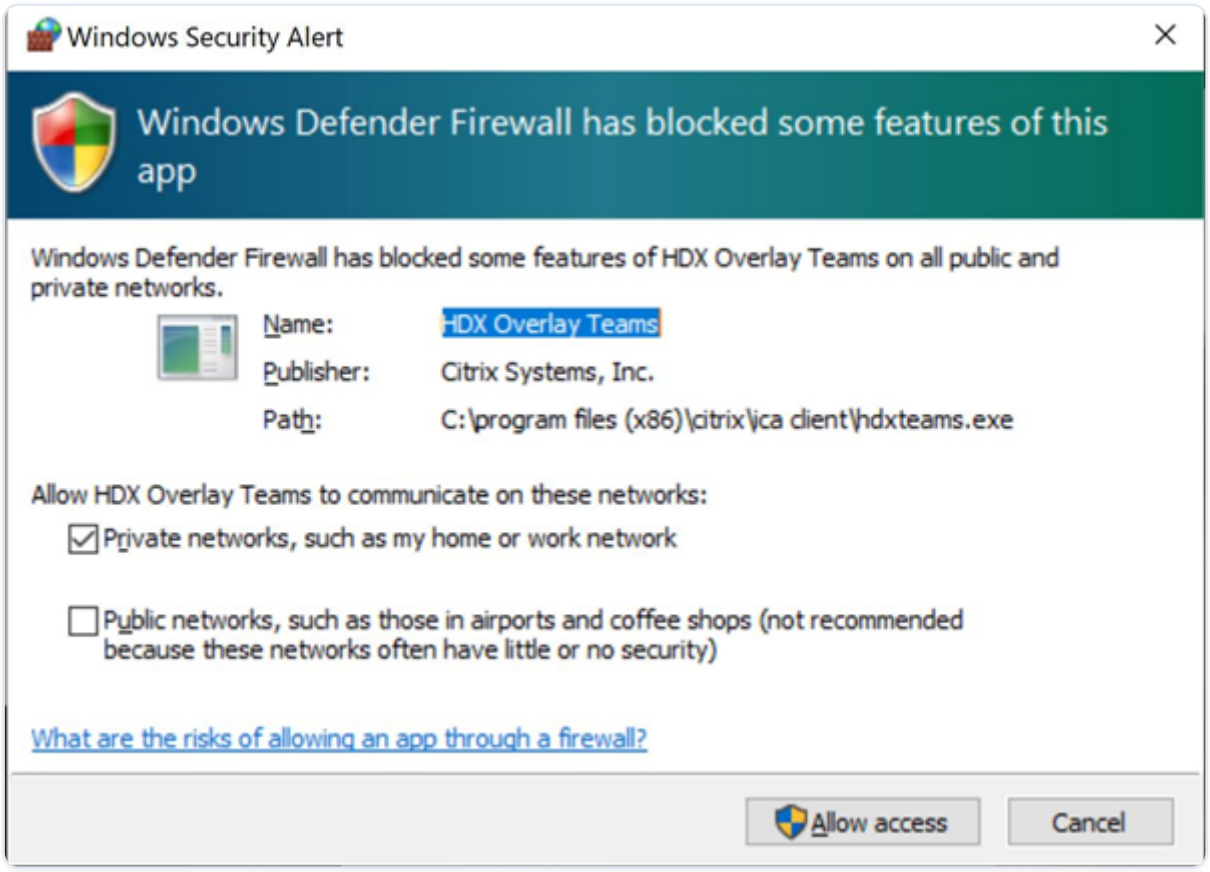
  - Subnet and WiFi-based locations are supported on the Workspace app for Windows, Linux, and Mac.

- Latitude and Longitude, if user permission is granted at the OS-level where Citrix Workspace app is installed.

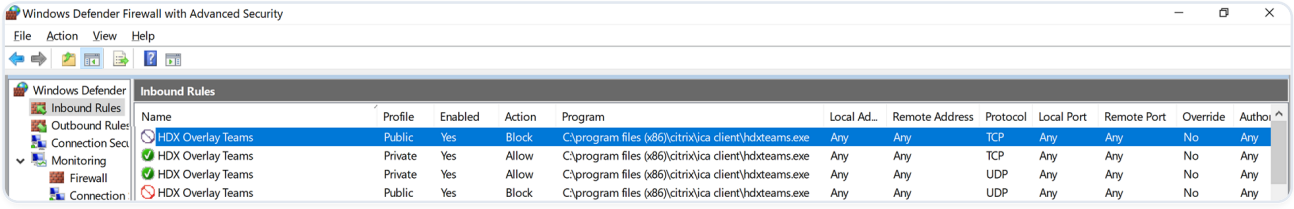
  - Supported on all Workspace app platforms. However, for Citrix Workspace app for Linux, you must include the `libgps` library in the OS distribution of the Thin Client (sudo apt-get install libgps23 gpsd lldpd).

Firewall considerations

When users start an optimized call using the Microsoft Teams client for the first time, they might notice a warning with the **Windows firewall** settings. The warning asks for users to allow communication for HdxTeams.exe or HdxRtcEngine.exe (HDX Overlay Microsoft Teams).



The following four entries are added under **Inbound Rules** in the **Windows Defender Firewall > Advanced Security** console. You can apply more restrictive rules if you want.



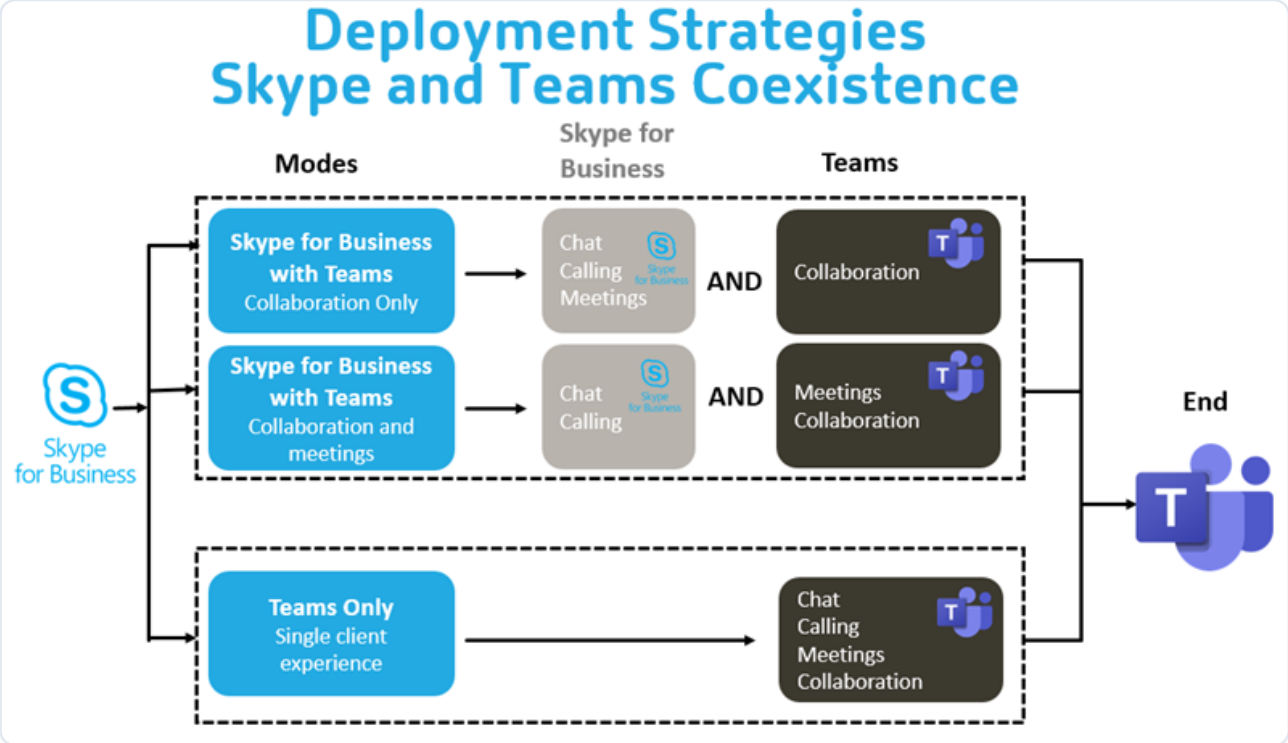
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Teams and Skype for Business Coexistence

You can deploy Microsoft Teams and Skype for Business side by side as two separate solutions with overlapping capabilities. For more information, see Understand Microsoft Teams and Skype for Business coexistence and interoperability.

Citrix RealTime Optimization Pack and HDX optimization for Microsoft Teams multimedia engines then honor the configuration set in your environment. Examples include island modes and Skype for Business with Microsoft Teams collaboration. Also, Skype for Business with Microsoft Teams collaboration and meetings.

Peripheral access can be granted only to a single application at the time. For example, webcam access by the RealTime Media Engine during a call locks the imaging device during a call. When the device is released, it becomes available for Microsoft Teams.



Citrix SD-WAN™: optimized network connectivity for Microsoft Teams

Optimal audio and video quality require a network connection to the Microsoft 365 cloud that has low latency, low jitter, and low packet loss. Backhauling of Microsoft Teams audio-video RTP traffic from Citrix Workspace app users at branch office locations to a data center before going to the internet can add excessive latency. It might also cause congestion on WAN links. Citrix SD-WAN optimizes connectivity for Microsoft Teams following Microsoft 365 network connectivity principles. Citrix SD-WAN uses the Microsoft REST-based Microsoft 365 IP address and web service and proximate DNS. This use is to identify, categorize, and steer Microsoft Teams traffic.

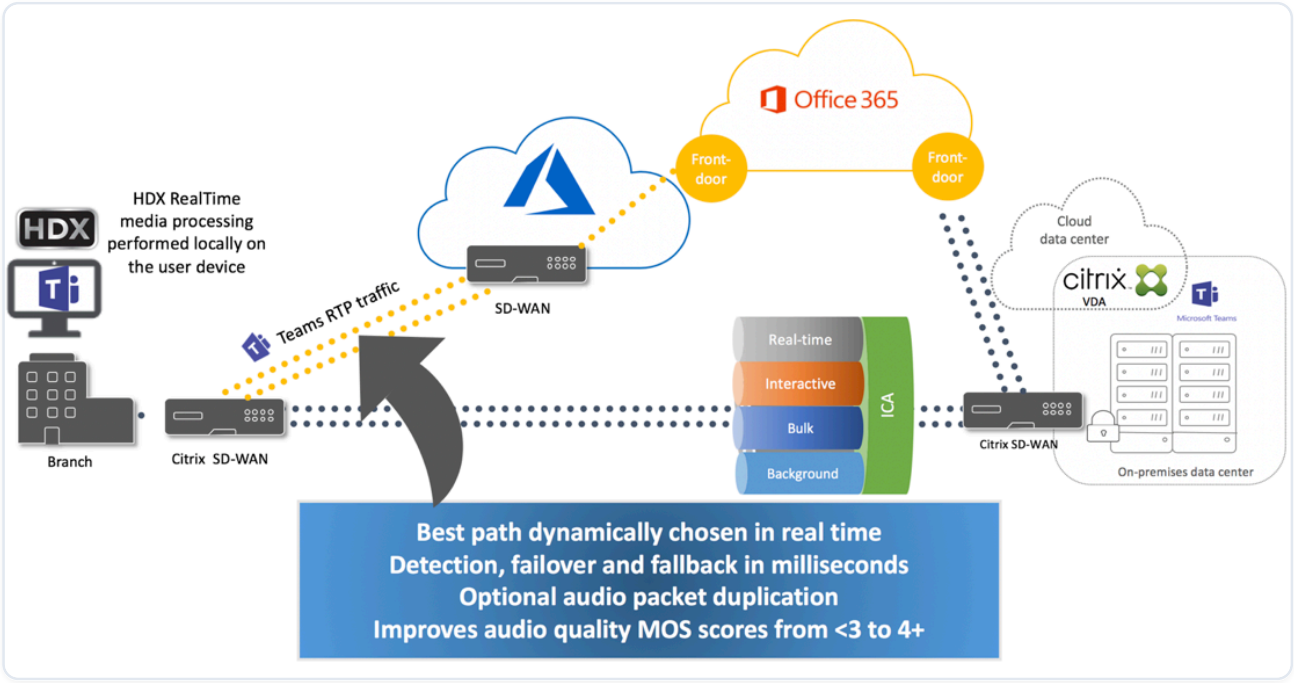
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Business broadband internet connections in many areas suffer from intermittent packet loss, periods of excessive jitter, and outages.

Citrix SD-WAN offers two solutions to preserve Microsoft Teams audio-video quality when network health is variable or degraded.

- If you use Microsoft Azure, a Citrix SD-WAN virtual appliance (VPX) deployed in the Azure VNET provides advanced connectivity optimizations. These optimizations include seamless link failover and audio packet racing.
- Citrix SD-WAN customers can connect to Microsoft 365 through the Citrix Cloud™ Direct service. This service provides reliable and secure delivery for all internet-bound traffic.

If the quality of the branch office internet connection isn't a concern, it might be enough to minimize latency. Steer Microsoft Teams traffic directly from the Citrix SD-WAN branch appliance to the nearest Microsoft 365 front door to minimize latency. For more information, see Citrix SD-WAN Office 365 optimization.



Multi-window meetings and chat

You can use multiple meetings or chat windows for Microsoft Teams in Windows. For details on the pop-out feature, see Microsoft Teams Pop-Out Windows for Chats and Meetings on the Microsoft 365 site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

This feature is supported with Citrix Workspace app for Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. It requires VDA 2112 or greater and was back-ported to 1912 CU6+ LTSR, and VDA 2112.

Background blurring and background effects

Citrix Workspace app for Windows, Mac, Linux, and ChromeOS/HTML5 supports background blurring and background effects in Microsoft Teams optimization with HDX.

You can either blur or replace the background with a default image and avoid unexpected distractions by helping the conversation stay focused on the silhouette (body and face). You can use this feature with P2P or conference calls.

NOTE:

This feature is integrated with the Microsoft Teams UI/buttons. MultiWindow support is a prerequisite that requires a VDA update to 2112 or later. For more information, see Multi-window meetings and chat.

Microsoft Teams UI controls on background blurring and effects require the following minimum versions:

- Citrix Workspace app for Windows 2207
- Citrix Workspace app for Mac 2301
- Citrix Workspace app for Linux 2212
- Citrix Workspace app for ChromeOS 2303

Limitations:

- The client must be connected to the internet while replacing the background image with a Microsoft Teams default image.
- Admin and user-defined background image replacement is not supported in the Microsoft Teams UI. Custom background images can be configured using configuration settings on the client, if the image is also stored on the client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Setting a custom background image

The following registry keys are only required if you don't plan to use the Microsoft Teams UI to control the feature, or if an admin wants to override default behaviors. For example, disable background blurring because the endpoint is not powerful enough.

On Windows

To set a custom background image, administrators or end-users must configure the following registry key on the client or endpoint:

Location: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Name: VideoBackgroundEffect
- Type: DWORD
- Value: 0 (disabled), 1 (enabled), 2 (background image replacement)

Value set to 1 blurs the background. This value can be set either by the end-user, or the administrator.

Value set to 2 also requires the **VideoBackgroundImage** key to be present as well. Only the administrator can set this value. The following key is required only if you want to replace the background image and not for blurring:

- Name: VideoBackgroundImage
- Type: REG_SZ
- Value: my_image_name.jpeg

The video background image must be present in the `C:\Program Files (x86)\Citrix\ICA Client` directory.

This registry configuration can also be used to enable background blurring or image replacement in Citrix Workspace app 2206 without the Microsoft Teams UI selector. In other words, if your environment or VDA doesn’t support multi-window, you can still apply the HKCU registry workaround with Citrix Workspace app 2206 or higher to achieve a similar result, although the user cannot control the functionality in the middle of the HDX session or Microsoft Teams call.

Registry key changes only take effect when the HDX session connects.

On Mac

User downloaded picture location: */Users/username/Downloads/any_image.png*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Run the following commands to set the custom image as the default image:

`defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2`

`defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"`

On Linux

User downloaded picture location: */home/username/Downloads/any_image.jpg*

Create file */var/.config/citrix/hdx_rtc_engine/config.json* and add the following configuration keys in JSON format. For example,

```
{


"VideoBackgroundEffect":2,


"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"


}
```

On HTML5

For HTML5, background blurring is only supported. Custom image replacement is not supported.

For background blurring, do the following:

1. Navigate to the **configuration.js** file in the **HTML5Client** folder.
2. Add the **backgroundEffects** attribute and set the attribute to **true**. For example,

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    }

}
```

3. Save the changes.

Client CPU Consumption considerations

While the blurring feature is frugal on the CPU, you can expect an increase in consumption. For example, on a thin client with a 4 Core, 1.5 GHz Intel® Pentium® Silver chip with TurboBoost up to 2.8 GHz, the background blurring adds about 2% to the CPU usage. Average CPU usage is less than 20%.

Gallery view and active speakers in Microsoft Teams

Microsoft Teams supports **Gallery**, **Large gallery**, and **Together mode** layouts.

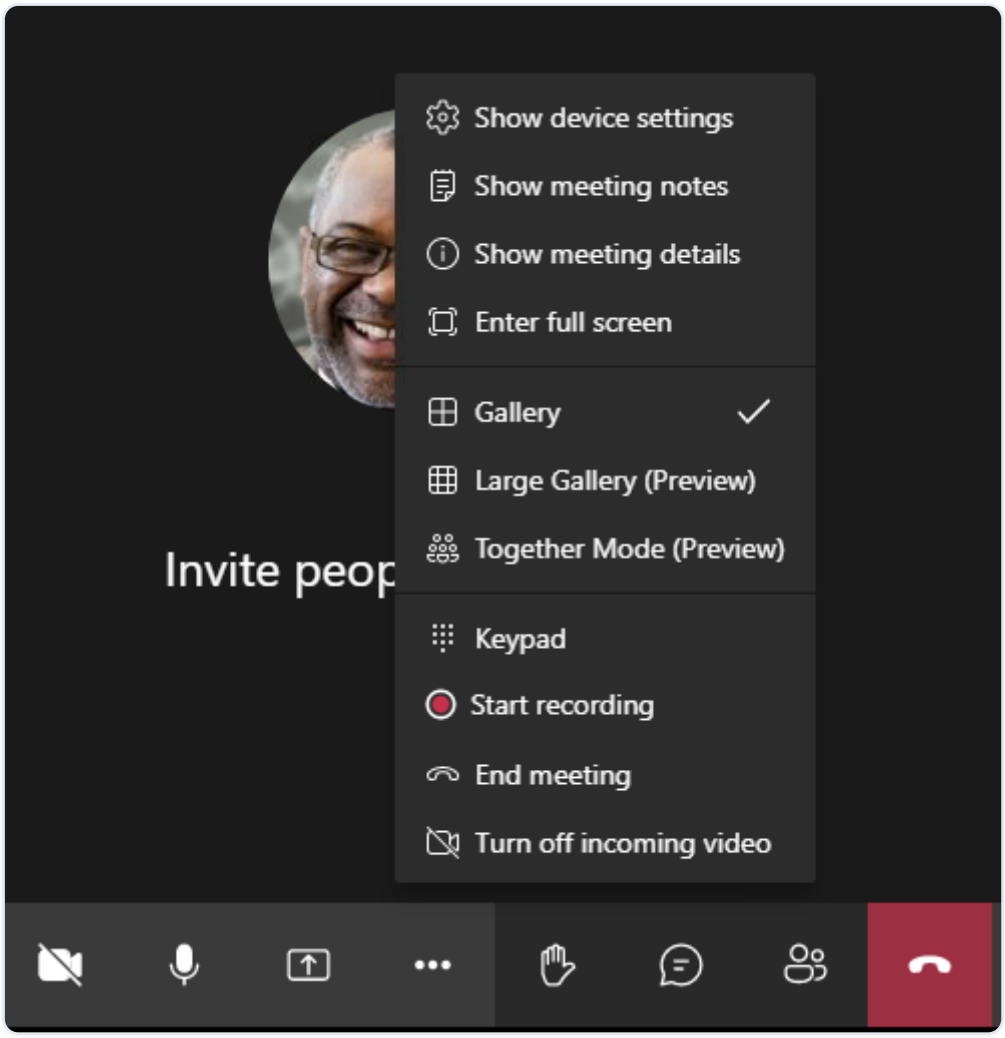
Microsoft Teams displays a 2x2 grid with video streams of four participants (known as **Gallery**). In this case, Microsoft Teams sends four video streams to the client device for decoding. When more than four participants share video, only the last four most active speakers appear on the screen.

Microsoft Teams also provides the large gallery view with a grid up to 7x7. As a result, the Microsoft Teams conference server composites a single video feed and sends it to the client device for decoding, resulting in lower CPU consumption. This single, matrix-style feed might include users' self-preview video as well.

Lastly, Microsoft Teams supports **Together mode**, which is part of the new meeting experience. Using AI segmentation technology to digitally place participants in a shared background, Microsoft Teams puts all participants in the same auditorium.

The user can control these modes during a conference call by selecting **Gallery**, **Large gallery**, or **Together mode** layouts in the ellipses menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Support for video aspect ratio constraints (CWA for Windows 2102, CWA for Linux 2106, CWA for MAC 2106 and later):

- The option **Fill to frame** is available in Gallery/Large Gallery View. This option crops the video size to fit it in the subwindow. **Fit to frame**, on the other hand, displays black bars (letterbox) on the sides of the video so there is no cropping.

The following table provides a comparison of Gallery and Large Gallery layouts:

	GALLERY VIEW 2X2 (DEFAULT)	LARGE GALLERY VIEW
Layout / Grid	Displays a 2x2 grid with video streams of four participants. Only the last four most active speakers appear on the screen and other participants do not appear on the grid.	Displays a 7x7 grid with video streams of 49 participants.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	GALLERY VIEW 2X2 (DEFAULT)	LARGE GALLERY VIEW
Mixing technique	A media router forwards individual streams from each participant to every user.	A central conference server mixes and transcodes all audio or video to create a tailored composite layout for every participant. This action introduces some additional latency.
Active speaker	The new active speaker replaces the least active speaker in the grid.	Displays all participants irrespective of whether they are active or inactive.
Encoding at the endpoint	One or more video streams might be encoded at the endpoint if Simulcast is enabled. For more information on Simulcast support, see Simulcast.	One or more video streams might be encoded at the endpoint if Simulcast is enabled. For more information on Simulcast support, see Simulcast.
Decoding at the endpoint	Each participant gets up to four individual media streams. This increases CPU consumption at the endpoint by HdxRtcEngine.exe (for decoding/rendering).	Each participant gets only a single stream for audio and video. This setting lowers the CPU consumption at the endpoint.
Maximum resolution	720p. When four participants are sharing video, the maximum resolution is 360p per video feed. If fewer than four participants are sharing video, then the resolution per video feed might be higher.	720p for the composite layout or mixing. There's no need for a high-quality video stream per participant in a composite layout. Because of this condition, each sender reduces resolution or upload bitrate.
'Slow-user' problem	Sender modifies each modality's (audio/video/ screenshare) quality to the lowest common network quality among the	Less susceptible to the lowest common network quality scenario. The conference server provides different qualities based on

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	GALLERY VIEW 2X2 (DEFAULT)	LARGE GALLERY VIEW
	participants. This multimedia stream is then forwarded to all other participants. As a result, a participant with poor network condition impacts the quality for everyone else in the call.	the network conditions of individual participants.
Self-preview	Displays yourself in a small thumbnail in real time.	Displays yourself in thumbnail and mixed with the rest of the video feeds. As a result, you might see yourself included in the main video layout with some additional delay.

Screen sharing in Microsoft Teams

Microsoft Teams relies on video-based screen sharing (VBSS), effectively encoding the desktop being shared with video codecs like H264 and creating a high-definition stream. With HDX optimization, incoming screen sharing is treated as a video stream.

Starting from Citrix Workspace app 2109 or higher for Windows, Linux, Mac, and Citrix Workspace app 2303 for ChromeOS users can share their screens and video camera simultaneously.

With earlier versions, if you're in the middle of a video call and the other peer starts to share the desktop, the original camera video feed is paused. Instead, the screen sharing video feed shows. The peer must then manually resume the camera sharing.

NOTE FOR POWERPOINT LIVE

This limitation does not exist if you're sharing content from PowerPoint Live. In that case, other peers can still see your webcam and content and navigate back and forth to review other slides. In this scenario, the slides are rendered on the VDA. To access a PowerPoint Live slide deck, click on the 'Share tray' button and select one of the suggested PowerPoint slides, or click 'Browse' and find a PowerPoint file on your computer or in OneDrive.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Outgoing screen sharing is also optimized and offloaded to Citrix Workspace app. In this case, the media engine captures and transmits only the Citrix Desktop Viewer (CDViewer.exe) window, with a red border drawn around it. Any local application overlapping with Desktop Viewer isn't captured.

NOTE

Set specific permission in Citrix Workspace app for Mac to enable screen sharing. For more information, see System Requirements.

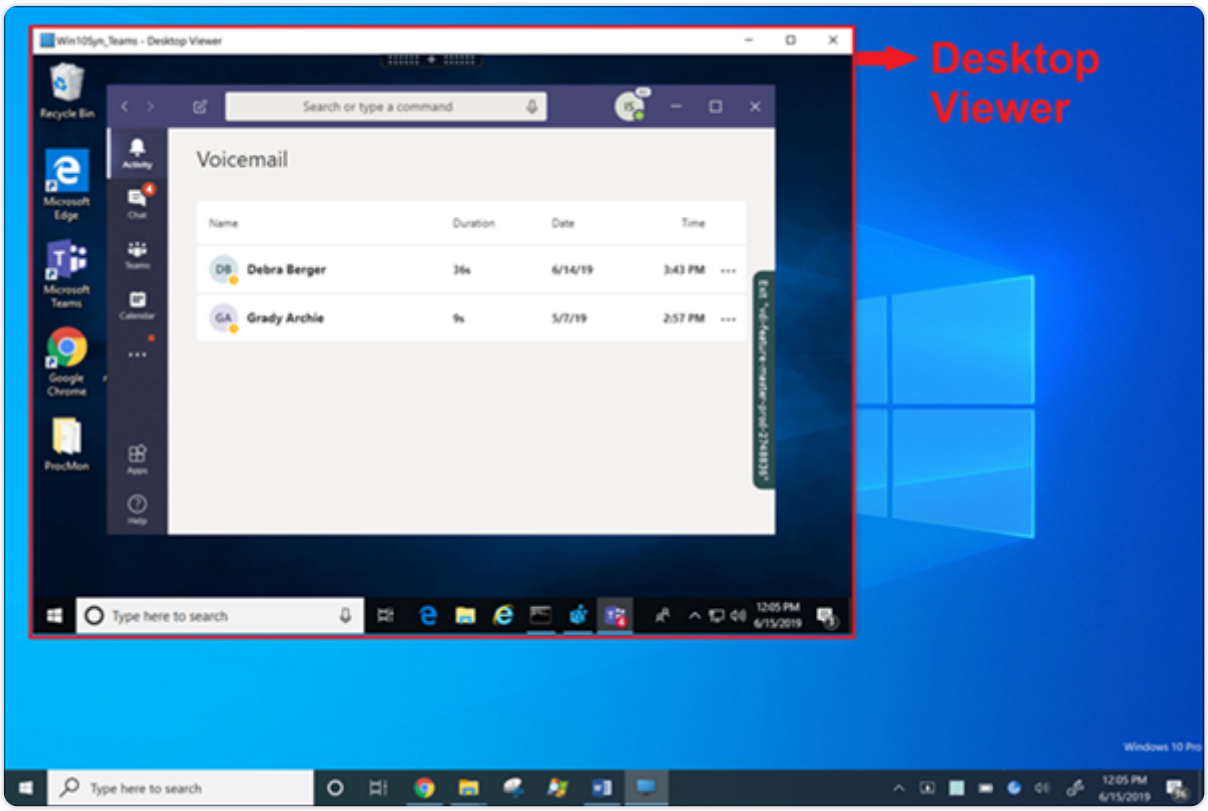
Multimonitor

If Desktop Viewer (CDViewer.exe) is in full-screen mode and spanning across multimonitor setups, Citrix Workspace app 2106 or later (Windows/Linux/Mac) allows the screen picker to select the monitor to share.

Known limitation:

- If Desktop Viewer is disabled or if Desktop Lock is being used, multimonitor selection isn't available in the Microsoft Teams screen picker. The Desktop Viewer might be disabled either by editing the `.ICA` file template or `StoreFront web.config`. SHIFT+F2 hotkey isn't compatible with multimonitor screen sharing.
- In Workspace app versions older than 2106, only the primary monitor is shared. Drag the application in the virtual desktop to the primary monitor for the other peer on the call to see it.
- Multimonitor screen sharing might not work if you configure the Citrix Workspace app with the virtual monitor layout feature (logical partition of a single physical monitor). In this case, all virtual monitors are shared as a composite image.
- Older versions of the Citrix Workspace app for Windows (1907 up to 2008) also shares a local application that runs in the client machine. This sharing is possible only if the local app was overlaid on top of Desktop Viewer. This behavior was removed in 2009.6 or higher, and 1912 CU5 or higher.
- While screen sharing, if you change from windowed mode to full-screen, screen sharing stops. You must stop and share again for screen sharing to work.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Screensharing from seamless application:

If you're publishing Microsoft Teams as a standalone, seamless application, screen sharing captures the local desktop of your physical endpoint. Citrix Workspace app minimum version 1909 is required.

App sharing

Starting with Citrix Workspace app for Windows 2112.1 and VDA 2112, Microsoft Teams supports app sharing.

Starting with Citrix Workspace app for Windows 2109, Mac 2203, Linux 2209, and VDA 2109, Microsoft Teams supports screen sharing of specific apps running in the virtual session. To share a specific app:

1. Navigate to the Microsoft Teams app within your remote session.
2. Click **Share content** in your Microsoft Teams UI.
3. Select an app to share in the meeting. The red border appears around an app you selected and the peers on the call can see the shared app.

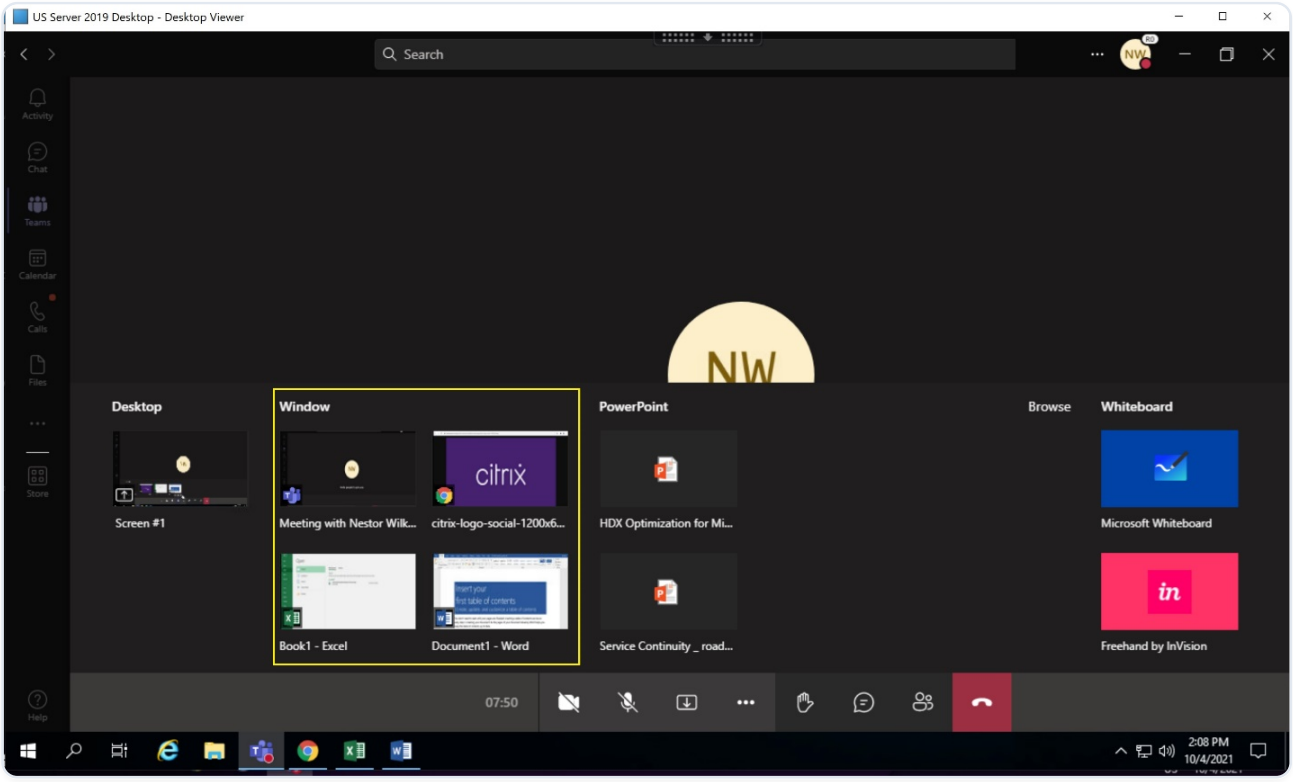
To share a different app, click **Share content** again and select a new app.

If you want to disable app sharing, create the following registry key on the VDA at `HKLM\SOFTWARE\Citrix\Graphics`: Name: `UseWsProvider` Type: `DWORD` Value: 0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.
- If you minimize an app, Microsoft Teams displays the last image from the shared app. You can maximize the window to resume screen sharing.
- Screen sharing depends on the VDA-side capturing of the window. The content is then relayed at a maximum rate to the Citrix Workspace app. The maximm rate is 30 frames per second. The Citrix Workspace app forwards the content to the peers or conference server.



Known limitations with screen sharing of specific app:

- Mouse pointer isn't visible when you are screen sharing an app.
- If you minimize an app when you're sharing it, only the app icon appears in the screen picker. The thumbnail of the app isn't previewed in the screen picker. You can't share the content and the red border does not appear until you maximize the app.
- LAA apps shows a list of apps that can be shared with desktop apps in the optimized Microsoft Teams in the VDA. However, when you select the app from the list, the result might not be as expected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compatibility with app protection The screen sharing of a specific app is compatible with the app protection feature in HDX optimized Microsoft Teams. You can screen share a specific app, if you've launched the app or desktop from a delivery group that has app protection enabled.

When you click **Share content** in the Microsoft Teams UI, the screen picker removes the **Desktop** option. You can only select the **Window** option to share any open app.

NOTE:

When you launch apps or desktops from a delivery group with app protection enabled, you aren't able to see the incoming video or screen sharing.

Give and Request control in Microsoft Teams

This feature is supported in the following versions of Citrix Workspace app (there is no dependency on the VDA version or Operative System, single session or multisession):

- Citrix Workspace app for Windows version 2112.1 and later
- Citrix Workspace app for Mac version 2203.1 and later
- Citrix Workspace app for Linux version 2203 and later
- Citrix Workspace app for ChromeOS version 2303 and later

You can request control during a Microsoft Teams call when a participant is sharing the screen. Once you have control, you can make selections, edits, or other keyboard and mouse activities to the shared screen.

To take control when a screen is being shared, click **Request control** button in the Microsoft Teams UI. The meeting participant who's sharing the screen can either allow or deny your request.

While you have control, you can make selections, edits, and other modifications to the shared screen. For these actions, you can use both keyboard and mouse. When you're done, click **Request control**.

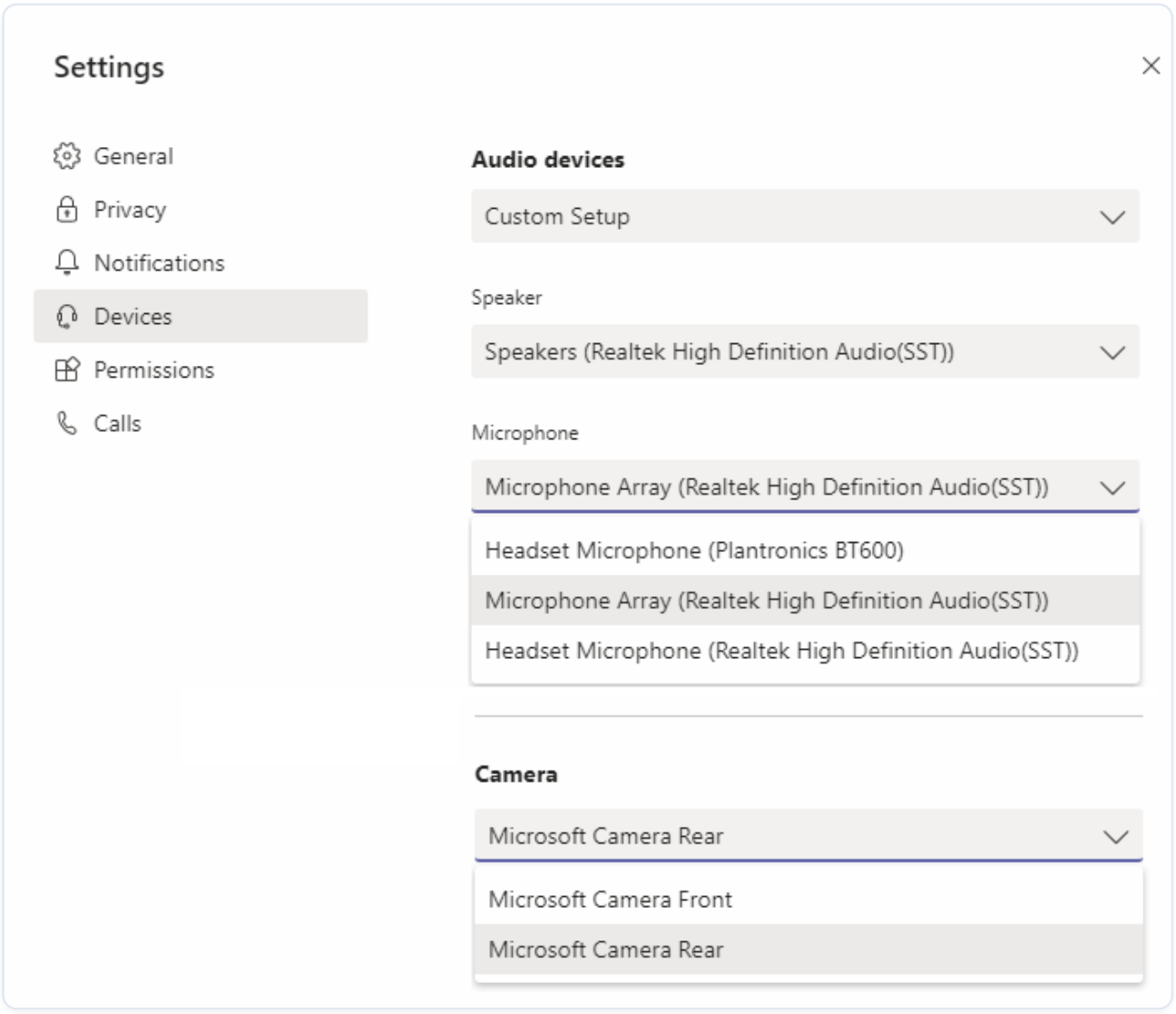
LIMITATIONS:

- Give and Request control are not available if the user is sharing a single app (also known as App sharing). The full desktop or monitor must be shared.
- The feature to pin the control bar to a specific location is not available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Peripherals in Microsoft Teams

When optimization for Microsoft Teams is active, the Citrix Workspace app accesses the peripherals (headsets, microphones, cameras, speakers, and so forth). Then the peripherals are properly listed in the Microsoft Teams UI (**Settings > Devices**).



Microsoft Teams does not access the devices directly. Instead, it relies on the Workspace app WebRTC media engine for acquiring, capturing, and processing the media. Microsoft Teams lists the devices for the user to select.

The peripherals that are inserted while Microsoft Teams is active aren't selected by default. You've to manually select the peripherals from the **Settings** > **Devices** screen of the Microsoft Teams UI. After the peripheral is selected, Microsoft Teams caches the information of the peripherals. As a result, the peripherals are automatically selected when you reconnect to a session from the same endpoint.

Recommendations:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microsoft Teams certified headsets with built-in echo cancellation. In setups with extra peripherals, where microphone and speakers are on separate devices, there might be an echo. An example is a webcam with a built-in microphone and a monitor with speakers. When using external speakers, place them as far as possible from the microphone. Also, place them away from any surface that might refract the sound into the microphone.
- Microsoft Teams certified cameras, although Skype for Business certified peripherals are compatible with Microsoft Teams.
- Citrix Workspace app media engine can't take advantage of CPU offloading with webcams that perform on-board H.264 encoding -UVC 1.1 and 1.5.

NOTE:

Workspace app 2009.6 for Windows can now acquire peripherals with audio formats with 24-bit or with frequencies above 96 kHz.

HdxTeams.exe (in the Citrix Workspace app for Windows 2009 or older) supports only these specific audio device formats (channels, bit depth, and sample rate):

- Playback Devices: up to 2 channels, 16 bit, frequencies up to 96,000 Hz
- Recording Devices: up to 4 channels, 16 bit, frequencies up to 96,000 Hz

Even if one speaker or microphone does not match the expected settings, device enumeration in Microsoft Teams fails and **None** displays under **Settings > Devices**.
Webrpc logs in **HdxTeams.exe** show this type of information:

```
Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...
Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!
```

As a workaround, disable the specific device or:

1. Open the **Sound Control Panel** (mmsys.cpl).
2. Select the playback or recording device.
3. Go to **Properties > Advanced** and change the settings to a supported mode.

Fallback mode

If Microsoft Teams fails to load in optimized VDI mode ("Citrix HDX Not Connected" in Teams/About/Version), the VDA falls back to legacy HDX technologies. The legacy HDX technologies might be webcam redirection and client audio and microphone redirection. If you're using a Workspace app version/platform OS that does not support Microsoft Teams optimization, fallback

© 1997–2026 Citrix Systems, Inc. All rights reserved.

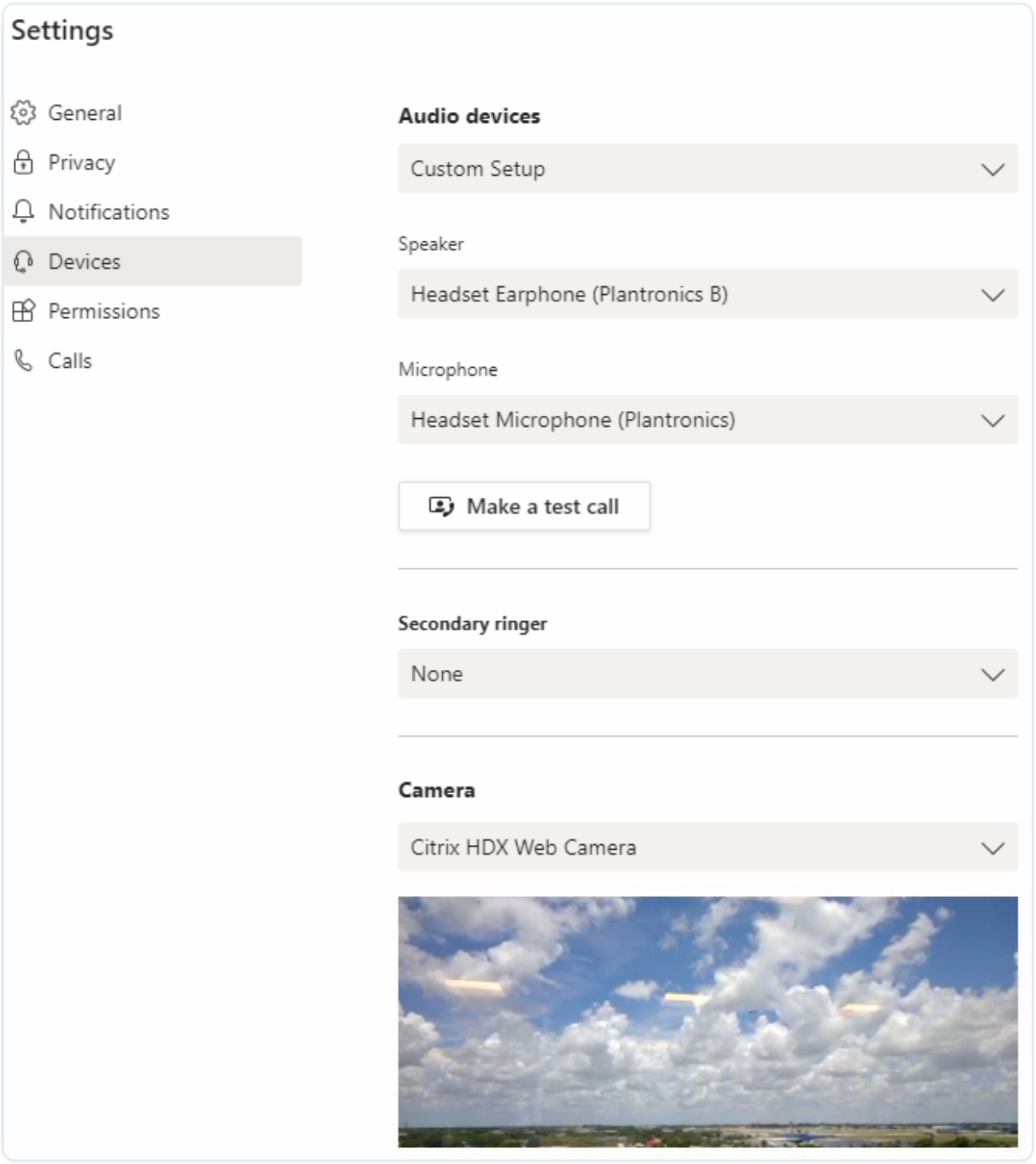
registry keys do not apply. In fallback mode, the peripherals are mapped to the VDA. The peripherals appear to the Microsoft Teams app as if they were locally attached to the virtual desktop.

You can now granularly control the fallback mechanism by setting the registry keys in the VDA. For information, see Microsoft Teams fallback mode in the list of features managed through the registry.

This feature requires Microsoft Teams version 1.3.0.13565 or later.

To determine if you are in optimized or unoptimized mode when looking at the **Settings > Devices** tab in the Microsoft Teams app, the main difference is the camera name. If Microsoft Teams loaded in unoptimized mode, legacy HDX technologies launch. The webcam name has the **Citrix HDX** suffix as shown in the following graphic. The speaker and microphone device names might be slightly different (or truncated) when compared to the optimized mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When legacy HDX technologies are used, Microsoft Teams doesn't offload audio, video, and screen sharing processing to the endpoint's Citrix Workspace app WebRTC media engine. Instead, HDX technologies use server-side rendering. Expect high CPU consumption on the VDA when you turn on video. Real-time audio performance might not be optimal.

Known limitations

Citrix limitations

Limitations on Citrix Workspace app:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HID buttons - Answer and end call aren't supported. Volume up and down are supported.
- QoS settings in the Admin Center for Microsoft Teams don't apply for VDI users.
- App protection add-on feature for the Citrix Workspace app prevents outgoing screen sharing and blocks incoming screen share and video.
- Users can't take screenshots of Microsoft Teams content while using a snipping tool on the VDA. However, if a snipping tool is used at the client side, the content can be captured.

Limitation on the VDA:

- When you configure the Citrix Workspace app High DPI setting to **Yes**, the redirected video window appears out of place. This limitation occurs when the monitor's DPI scaling factor is set to anything above 100%.

Limitations on Citrix Workspace app and the VDA:

- You can only control the volume of an optimized call using the volume bar on the client machine -- not on the VDA.

Simulcast

Simulcast support is enabled for optimized Microsoft Teams video conference calls on Windows and Mac. For Linux check with your thin client vendor. With Simulcast the quality and experience of video conference calls across different endpoints are improved by adapting to the proper resolution for the best call experience for all callers.

With this improved experience, each user might deliver multiple video streams in different resolutions (for example, 720p, 360p, and so on) depending on several factors including endpoint capability, network conditions, and so on. The receiving endpoint then requests the maximum quality resolution that it can handle thereby giving all users the optimum video experience.

NOTE:

This feature is available only after the roll-out of an update from Microsoft Teams. For information on ETA, `<https://www.microsoft.com/>` go to and search for Microsoft 365 roadmap. When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft limitations

- A 3x3 gallery view isn't supported. Microsoft Teams dependency – contact Microsoft for when to expect a 3x3 grid.
- Interoperability with Skype for Business is limited to audio calls, no video modality.
- Incoming and outgoing video stream maximum resolution is 720p. Microsoft Teams dependency – contact Microsoft for when to expect 1080p.
- PSTN call ringback tone isn't supported.
- Media bypass for Direct Routing isn't supported.
- Broadcast and live event producer and presenter roles aren't supported. Attendee role is supported but not optimized (renders on the VDA instead).
- The zoom in and zoom out function in Microsoft Teams isn't supported.
- Location-Based Routing and Media Bypass are not supported.
- Call merge is not supported (option not displayed in the user interface).

Citrix and Microsoft limitations

- When doing screen sharing, the option **include system audio** isn't available.
- Simulcast isn't supported on ChromeOS.

Upcoming Microsoft Teams Single-Window EOL

On January 31, 2024, Microsoft will retire the Microsoft Teams support for Single-window UI when using VDI Microsoft Teams optimization and support only the Multi-Window experience. Microsoft gave notice of this deprecation on 9/8/2023 in the M365s Admin Center (Post ID: MC674419). Public details about the Multi-Window feature can be found in the Tech Community article: New Meeting and Calling Experience in Microsoft Teams.

You must upgrade your VDA and Citrix Workspace app to the supported versions to continue using Microsoft Teams in optimized mode for video and screen sharing. If you don't upgrade your infrastructure and endpoints to support multi-window, you can only establish audio calls. You will not be able to use the optimized video and screensharing functionality.

The following table illustrates the minimum, LTSR, and recommended versions of VDA and Citrix Workspace app required to continue using optimized calling in Microsoft Teams on Citrix VDI:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPONENT	MINIMUM VERSION	LTSR SUPPORTED VERSION	RECOMMNDED VERSION
Microsoft Teams	1.5.00.11865	Not applicable	Latest
VDA	1912 CU6 LTSR, 2203 LTSR, 2112 CR	1912 CU7+, 2203 CU2+	2308 CR+
Citrix Workspace app for Windows	2205 CR	2203 CU2+	2309 CR+
Citrix Workspace app for Mac	2209 CR	Not applicable	2308 CR+
Citrix Workspace app for Linux	2209 CR	Not applicable	2308 CR+
Citrix Workspace app for ChromeOS or HTML5	2303 CR	Not applicable	2309 CR+

Deprecation announcement of the SDP format (Plan B) from WebRTC

Citrix is planning to deprecate the current SDP format (Plan B) support from WebRTC in future releases. You must use Unified Plan in WebRTC to support optimized Microsoft Teams functionalities.

Products that are affected

In one of the future releases of the Citrix Workspace Application, calls between endpoints with the upcoming release for the Citrix Workspace app and endpoints with Citrix Workspace app 2108 or older versions will not be supported. This calling incompatibility includes 1912 LTSR Citrix Workspace app clients (CWA). The following CWA clients are impacted:

- Citrix Workspace app for Windows
- Citrix Workspace app for Linux
- Citrix Workspace app for Mac
- Citrix Workspace app for Chrome

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Replacement for Plan B

If you are running the Citrix Workspace app version older than 2109, you must upgrade to a supported version (preferably the latest CR release). Otherwise, any calls with a future release or newer endpoints fail to connect. Calls between future releases and your federated communication partners might also fail to complete if the federated partner has not upgraded their Citrix Workspace app.

Citrix Workspace app version 2108 has completed its' support date in March 2023 and must be upgraded to a newer version. For more information, see Workspace App for details on Citrix Workspace app version support.

For more information on the Plan B deprecation, see the WebRTC documentation.

Additional information

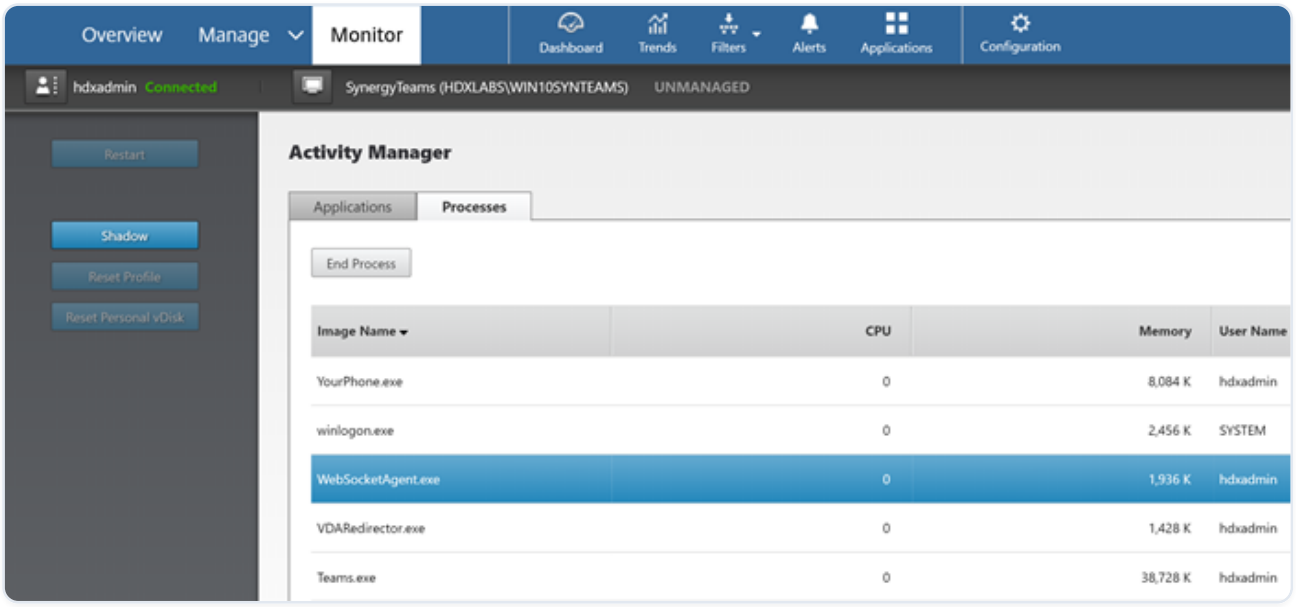
- Monitor, troubleshoot, and support Microsoft Teams
- Deploy the Microsoft Teams desktop app to the VM
- Install Microsoft Teams using MSI (VDI Installation section)
- Thin clients
- Skype for Business Network Assessment Tool
- Understand Microsoft Teams and Skype for Business coexistence and interoperability

Monitor, troubleshoot, and support Microsoft Teams

Monitor Teams

This section provides guidelines for monitoring Microsoft Teams optimization with HDX. If you're running in optimized mode and `HdxRtcEngine.exe` is running on the client machine, a process on the VDA called `WebSocketAgent.exe` is running in the session. Use the **Activity Manager** in Director to see the application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



With the VDA minimum version 1912, you can monitor active Teams calls using the Citrix HDX Monitor (minimum version 3.11). The Citrix Virtual Apps and Desktops product ISO contains the latest `hdxmonitor.msi` in the folder `layout\image-full\Support\HDX Monitor`.

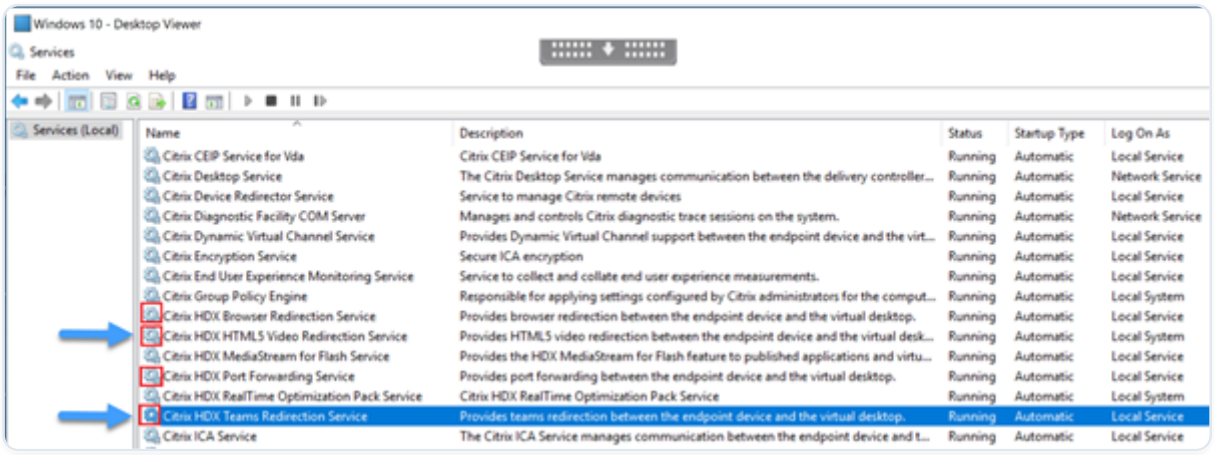
For more information, see *Monitoring* in the Knowledge Center article CTX253754.

Troubleshoot

This section provides troubleshooting tips for issues that you might encounter when using optimization for Microsoft Teams. For more information, see CTX253754.

On the Virtual Delivery Agent

There are four services installed by BCR_x64.msi. Only two are responsible for Microsoft Teams redirection in the VDA.



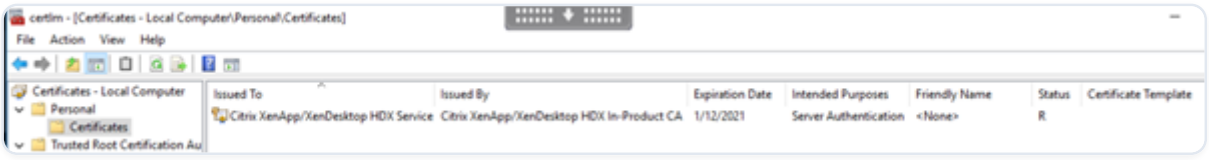
- **Citrix HDX Teams Redirection Service** establishes the virtual channel used in Microsoft Teams. The service relies on CtxSvcHost.exe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

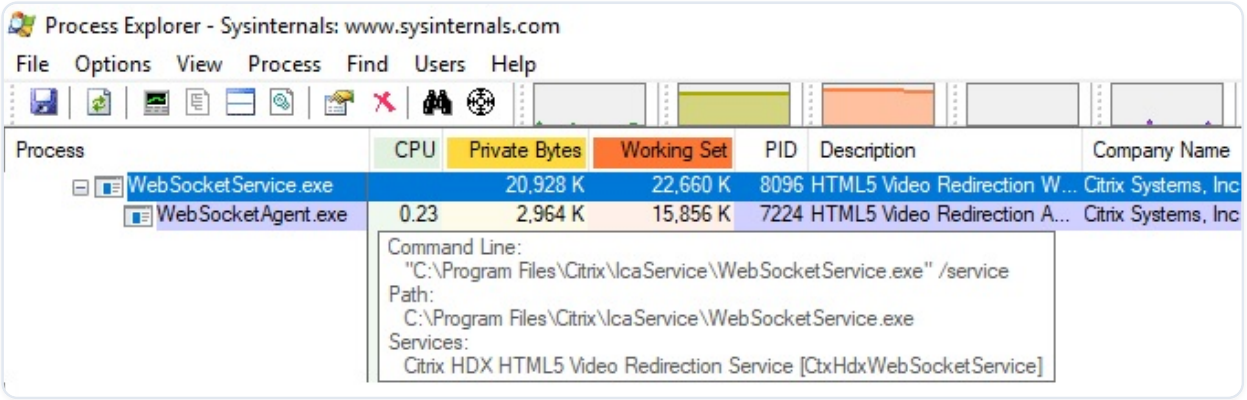
- **Citrix HDX HTML5 Video Redirection Service** runs as WebSocketService.exe listening on 127.0.0.1:9002 TCP. WebSocketService.exe performs two main functions:

  i. **TLS termination for secure WebSockets** receives a secure WebSocket connection from vdiCitrixPeerConnection.js, which is a component inside the Microsoft Teams app. You can track it with the Process Monitor. For more information about certificates, see the section "TLS and HTML5 video redirection, and browser content redirection" under Communication between Controller and VDA.

  Some antivirus and desktop security software interferes with the proper functioning of `WebSocketService.exe` and its certificates. While the Citrix HDX HTML5 Video Redirection service might be running in the `services.msc` console, the localhost `127.0.0.1:9002` TCP socket is never in listening mode as seen in netstat. Trying to restart the service causes it to hang ("Stopping…"). Ensure you apply the proper exclusions for the `WebSocketService.exe` process.



  ii. **User session mapping.** When the Microsoft Teams application starts, WebSocketService.exe starts the WebSocketAgent.exe process in the user's session in the VDA. WebSocketService.exe runs in Session 0 as a LocalSystem account.



  You can use **netstat** to check if the WebSocketService.exe service is in an active listening state in the VDA.

  Run `netstat -anob -p tcp` from an elevated command prompt window:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

  On a successful connection, the state changes to ESTABLISHED:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

IMPORTANT:

WebSocketService.exe listens in two TCP sockets, 127.0.0.1:9001 and 127.0.0.1:9002. Port 9001 is used for browser content redirection and HTML5 video redirection. Port 9002 is used for Microsoft Teams redirection. Ensure that you don"t have any proxy configurations in the Windows OS of the VDA that can prevent a direct communication between Teams.exe and WebSocketService.exe. Sometimes, when you configure an explicit proxy in Internet Explorer 11 (**Internet Options > Connections > LAN settings > Proxy Server**), connections might flow through an assigned proxy server. Verify that **Bypass proxy server for local addresses** is checked when using a manual and explicit proxy setting.

Services locations and descriptions

SERVICE	PATH TO EXECUTABLE IN WINDOWS SERVER OS	LOG ON AS	DESCRIPTION
Citrix HTML5 Video Redirection Service	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	Local System account	Provides multiple HDX Multimedia services with the initial framework required to perform media redirection between the virtual desktop and the endpoint device.
Citrix HDX Browser Redirection Service	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	This account (local service)	Provides browser content redirection between the endpoint device and the virtual desktop.
Citrix Port Forwarding Service	"C:\Program Files (x86)\Citrix\System3	This account (local service)	Provides port forwarding between the endpoint device and the virtual

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SERVICE	PATH TO EXECUTABLE IN WINDOWS SERVER OS	LOG ON AS	DESCRIPTION
	2\CtxSvcHost.exe" -g PortFwdSvcs		desktop for browser content redirection.
Citrix HDX Teams Redirection Service	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	Local System account	Provides Microsoft Teams redirection between the endpoint device and the virtual desktop.

Citrix Workspace™ app

On the user's endpoint, the Citrix Workspace app for Windows instantiates a new service called HdxTeams.exe. It does so when Microsoft Teams launches in the VDA and the user tries to call or access the peripherals in self-preview. If you don't see this service, check the following:

1. Ensure that you installed as a minimum the Workspace App version 1905 for Windows. Do you see HdxTeams.exe and the webrpc.dll binaries in the Workspace app installation path?
2. If you validated step1, do the following to check if HdxTeams.exe is getting launched.
    a. Exit Microsoft Teams on the VDA.
    b. Start services.msc on VDA.
    c. Stop the Citrix HDX Teams Redirection Service.
    d. Disconnect the ICA® session.
    e. Connect the ICA session.
    f. Start the Citrix HDX Teams Redirection Service.
    g. Restart the Citrix HDX HTML5 Video Redirection Service.
    h. Launch Microsoft Teams on the VDA.
3. If you still don't see HdxTeams.exe being launched on the client endpoint, do the following:
    a. Restart the VDA.
    b. Restart the client endpoint.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support

Citrix and Microsoft jointly support the delivery of Microsoft Teams from Citrix Virtual Apps and Desktops™ using optimization for Microsoft Teams. This joint support is the result of close collaboration between the two companies. If you have valid support contracts and you experience an issue with this solution, open a support ticket with the vendor whose code you suspect to be causing the issue. That is, Microsoft for Teams or Citrix for the optimization components.

Citrix or Microsoft receives the ticket, triages the issue, and escalates as appropriate. There is no need for you to contact each company's support team.

When you have a problem, we recommend you click **Help > Report a Problem** in the Teams UI. VDA-side logs are automatically shared between Citrix and Microsoft to resolve technical issues faster.

Collecting logs

HDX media engine logs can be found on the user's machine (not on the VDA). In case of any issues, make sure you attach logs to your support case.

Windows logs:

You can locate Windows logs at %TEMP% inside the **HDXTeams** folder (AppData/Local/Temp/HDXTeams or AppData/Local/Temp/HdxRtcEngine). Look for a .txt file called webrpc_Day_Month_timestamp_Year.txt. If you are using newer versions of Citrix Workspace app, for example Citrix Workspace app 2009.5 or later, store the logs in AppData\Local\Temp\HdxRtcEngine.

Each session creates a separate folder for logs.

Mac logs:

1. VDWEBRTC log - records the execution of the virtual channel.

   Location：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngine log - records the execution of the processes on HdxRtcEngine.

   Location: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   HdxRtcEngine log is enabled by default.

3. Webrpc logs - are the most important logs that record the execution of the wrap-up of the webrtc library.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Location: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linux logs:

You can locate Linux logs in the `/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/` folders. Webrtc log: `/tmp/webrpc/<current date>/webrtc.log` Kernel log: `/var/log/syslog`

ICE/STUN/TURN/ logs:

When establishing a call, these four ICE phases are required:

- Candidate gathering
- candidate exchange
- Connectivity checks (STUN bind requests)
- Candidate promotion

In the HdxRtcEngine.exe logs, the following entries are the relevant Interactive Connectivity Establishment (ICE) entries. These entries must be there for a call set-up to succeed. See the following sample snippet for the gathering stage:

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

If there are multiple ICE candidates, the order of preference is:

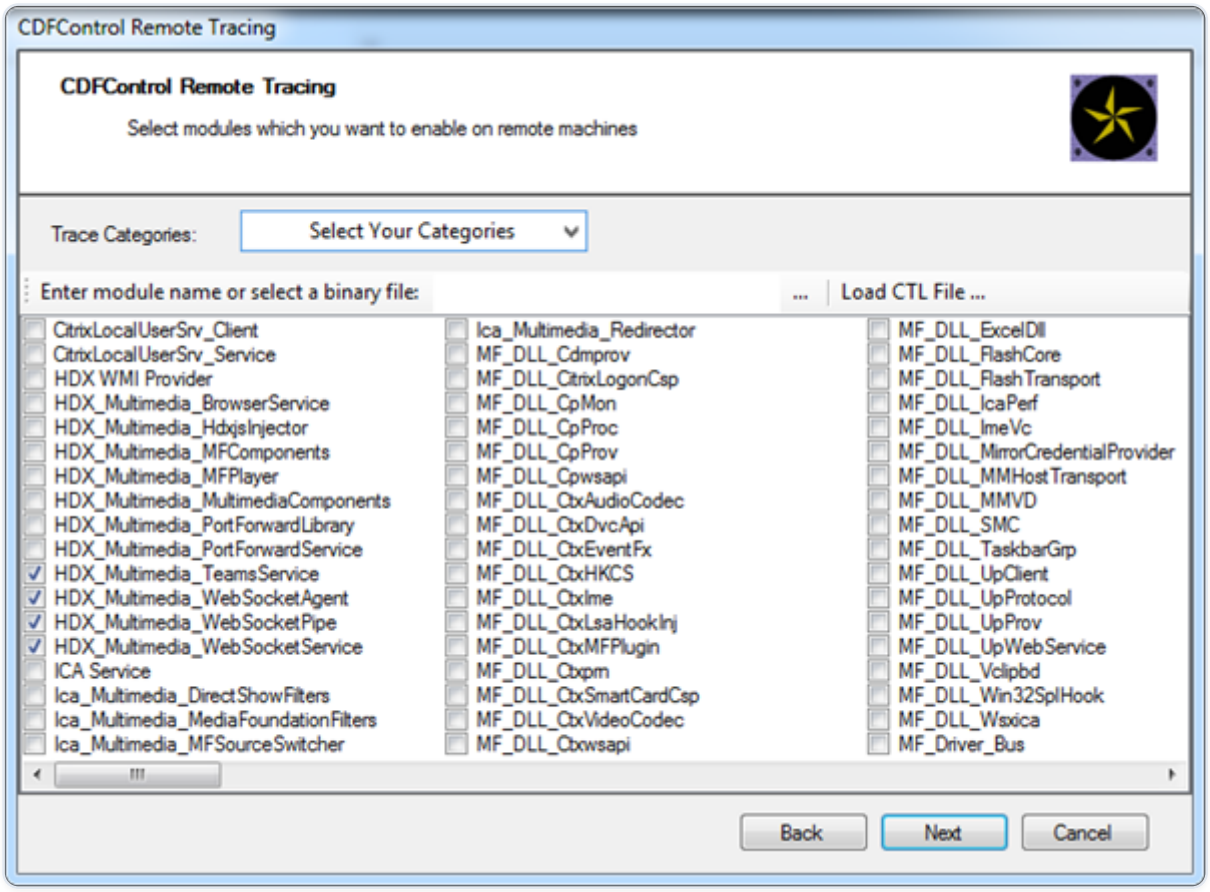
1. host
2. peer reflexive
3. server reflexive
4. transport relay

If you encounter an issue and can reproduce it consistently, we recommend that you click **Help > Report a problem** in Teams. Logs are shared between Citrix and Microsoft to resolve technical issues if you opened a case with Microsoft. Capturing CDF traces before contacting Citrix Support is also beneficial. For more information, see the Knowledge Center article CDFcontrol.

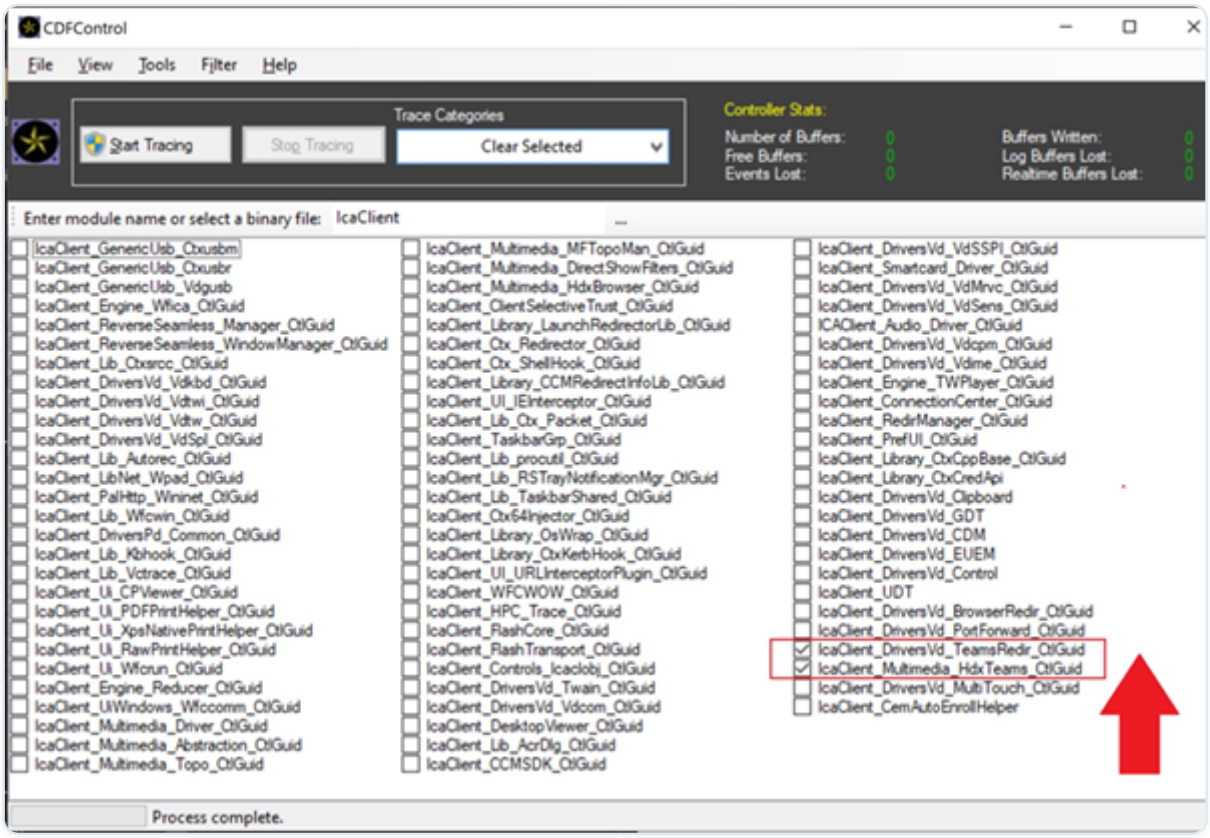
For recommendations for collecting CDF Traces, see the Knowledge Center article Recommendations for Collecting the CDF Traces.

VDA side CDF traces - Enable the following CDF trace providers:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Workspace app side CDF traces - Enable the following CDF trace providers:



- IcaClient_DriversVd_TeamsRedir (optional)
- IcaClient_Multimedia_HdxTeams (requires Citrix Workspace app 2012 or later)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows Media redirection

Windows Media redirection controls and optimizes the way servers deliver streaming audio and video to users. By playing the media run-time files on the client device rather than the server, Windows Media redirection reduces the bandwidth requirements for playing multimedia files. Windows Media redirection improves the performance of Windows Media Player and compatible players running on virtual Windows desktops.

If the requirements for Windows Media client-side content fetching are not met, media delivery automatically uses server-side fetching. This method is transparent to users. You can use the Citrix Scout to perform a Citrix Diagnosis Facility (CDF) trace from HostMMTransport.dll to determine the method used. For more information see, Citrix Scout.

Windows Media redirection intercepts the media pipeline at the host server, captures the media data in its native compressed format, and redirects the content to the client device. The client device then recreates the media pipeline to decompress and render the media data received from the host server. Windows Media redirection works well on client devices running a Windows operating system. Those devices have the multimedia framework required to rebuild the media pipeline as it existed on the host server. Linux clients use similar open-source media frameworks to rebuild the media pipeline.

The policy setting **Windows Media Redirection** controls this feature and is **Allowed** by default. Usually, this setting increases audio and video quality rendered from the server to a level that is comparable to content played locally on a client device. In the rare cases, media playing using Windows Media redirection appears worse than media rendered using basic ICA® compression and regular audio. You can disable this feature by adding the **Windows Media Redirection** setting to a policy and setting its value to **Prohibited**.

For more information about the policy settings, see Multimedia policy settings.

Limitation:

When you’re using Windows Media Player and Remote Audio & Video Extensions (RAVE) enabled inside a session, a black screen might appear. This black screen might appear if you right-click on the video content and select **Always show Now Playing on top**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual Channel Plugin Manager

Introduction

Virtual channel plugin manager is designed to deploy plugins across client endpoints for specified applications. The plugin manager detects specific applications running on the VDA and prompts the user to install the plugin on the endpoint to achieve the best experience when running the application.

Users can choose to install the plugin, skip it or deny the installation. The plugin manager provides flexibility to manage the plugins on all endpoints - managed or unmanaged

For Example: Microsoft Teams has a new architecture (SlimCore Optimization), that requires a plugin to be installed on the endpoints for the optimization to work. The Virtual channel plugin manager can deploy the plugins across your endpoints. For more information, see new VDI solution for Teams

System Requirements

Following are the minimum requirements for Virtual channel plugin manager.

- Virtual Desktop Agent (VDA)
  - 2411 CR
  - 2402 LTSR CU2
- DDC
  - Cloud 121 Release
  - 2407 CR
  - 2402 LTSR CU1
- Citrix Workspace™ App (Citrix Workspace App)
  - Citrix Workspace App for Windows 2409

NOTE:

This feature is currently applicable to Windows endpoints.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported applications

- Currently supported applications are listed below:
    - Microsoft Teams - See new VDI solution for Teams

Virtual Channel Plugin Manager overview

Understanding the Feature

Citrix® understands the customers' environments can be complex and deploying a plugin across managed and unmanaged endpoints requires significant effort. This feature is designed to simplify the process.

This feature includes two components:. One on the VDA side (detector process) and another on the Citrix Workspace™ App side (installer process). When administrators meet the prerequisites mentioned above, such as enabling policies, making registry entries and specifying an application to monitor:

- The VDA side detector process monitors for the application launch by the end user once they logon to the Virtual desktop
- The detector process informs the Citrix Workspace App side to prompt the user to install the plugin necessary to optimize the specified application
- Users receive a pop-up on their screen with brief details about the plugin. Users can choose to install the plugin, skip or choose to never install it
    - If users skip the installation process, they will not see the pop-up again in that session. The installation prompt will appear upon session reconnect.
    - If users choose to never install the plugin, the choice will be logged in their user profile for administrator visibility.
- If users choose to install the plugin, the Citrix Workspace App side will download and install the plugin on the endpoint.
    - On successful installation, the user will be shown a message to reconnect the session for the plugin to take effect. The user can choose to do it immediately or close the success message and do a reconnect later.
    - If the installation fails, the user will see an error message and the failure will be logged for administrator visibility.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual Channel Plugin Manager Configuration

Deployment

1. Check if the Microsoft Teams redirection policy is enabled: Refer Microsoft Teams redirection policy for more details.

   This policy must be enabled regardless of the application being monitored. In the future, if more applications are supported and you want to monitor those applications instead of Microsoft Teams, this policy must still be enabled. Note that this policy is enabled by default.

2. Virtual channel plugin manager policy must be enabled: Refer Virtual channel plugin manager policy settings for detailed instructions on how to enable the policy.

   This policy is available in the Multimedia Policy Settings on Citrix Studio. Enabling the policy allows you to specify the application name to be monitored For Example., “Microsoft Teams”. This policy is disabled by default.

3. Citrix Workspace™ app must be installed in system wide mode.

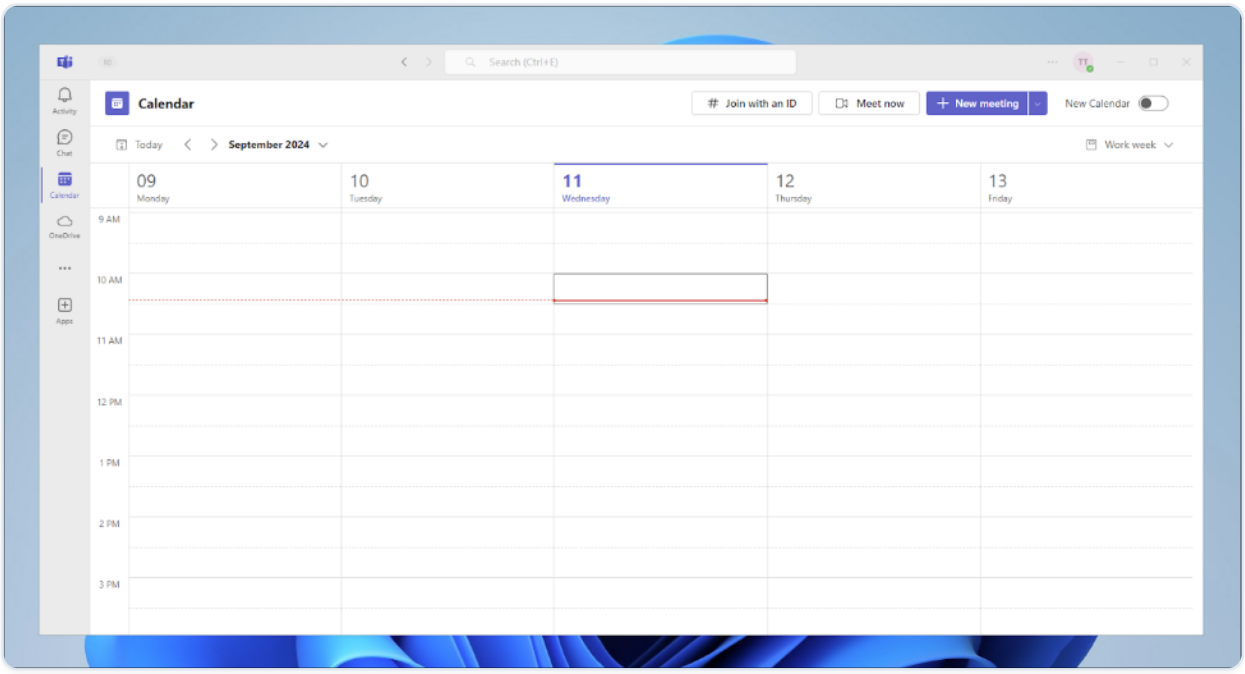
NOTE:

The plugins are downloaded to the endpoint from the third party CDN. For example, if you select Microsoft Teams, the plugin will be downloaded from the Microsoft CDN. Therefore, the endpoint must have access to the third party CDN. Otherwise, the plugin installation will fail.

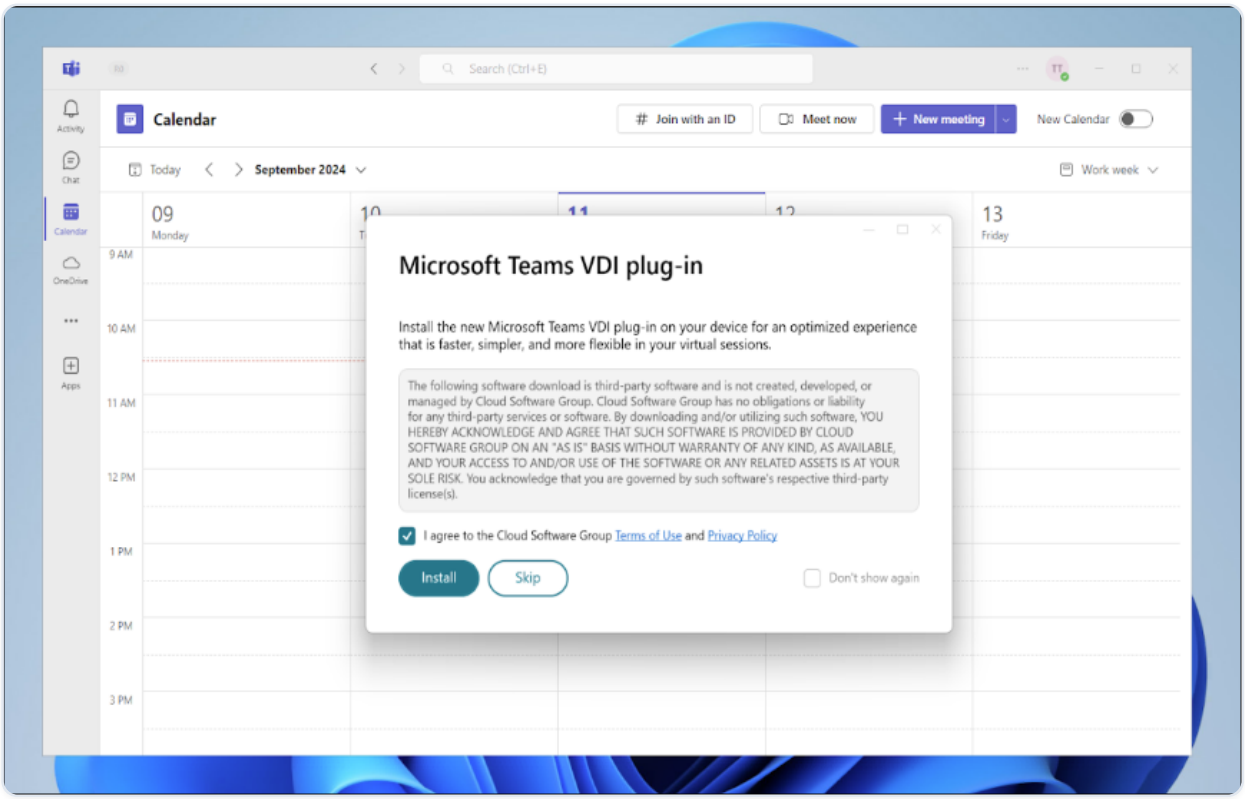
Procedure

1. User launches application on the Citrix session. For e.g., Microsoft Teams.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

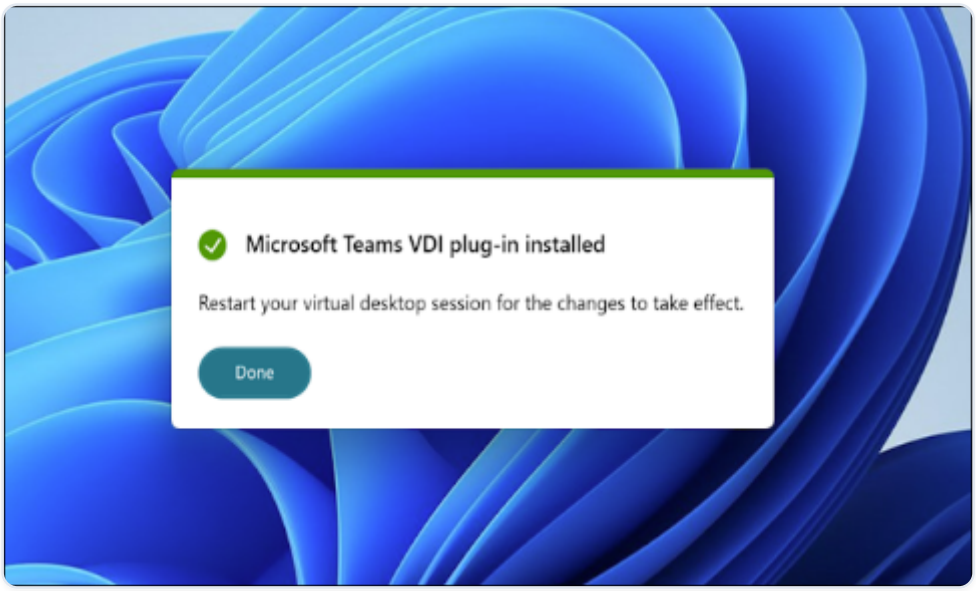


2. User receives a pop up to install the Teams VDI plugin on the endpoint for better experience. The pop up is above the session and not inside the session as the plugin will be installed on the endpoint.



3. User clicks on the install button and the plugin is installed. Users need to restart the virtual desktop session for the changes to take effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Known Issues & Limitations

- In 2407 VDA, the following registry setting needs to be set to 1 on the VDA in addition to the policy for the feature to be activated. This registry setting is automatically allowed and not required to be configured from 2411 VDA

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

  Name: EnableAppDetector Type: DWORD`
- More limitations to be added

Unified Communications SDK Optimization

Introduction

Citrix Virtual Apps and Desktops lets you deliver applications to your users on a wide variety of endpoint devices. Many of these applications include real-time communication (RTC) features, like audio and video conferencing. However, challenges can arise when delivering these applications in a virtualized environment. Traditional delivery methods route media streams (audio/video) from the client device to the VDI server in the data center before sending them back to the endpoint. This "hairpinning" introduces unnecessary traffic and processing overhead on the server, especially for bandwidth-intensive audio & video calls.

The Citrix Unified Communications SDK (UCSDK) is a technology that allows technology vendors to optimize these RTC applications for use in Citrix environments. When an application is optimized, it can provide a user experience that matches or even exceeds that of the application running on a local desktop. In today's world, seamless real-time communication is essential for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

productivity and collaboration. When using applications within a virtual environment, it's crucial that audio and video calls, screen sharing, and other communication features work as smoothly as they would on a local desktop. Optimized applications deliver this experience.

This product documentation details all that is needed for the Citrix customers to learn and deploy UCSDK optimized applications.

How it works

Citrix offers an optimized delivery method for real-time communication applications within VDIs. This approach leverages the Unified Communications SDK (UCSDK) to split the virtualized application into two parts:

- **User Interface (UI):** The user interface remains within the virtual host, displayed seamlessly within the virtual desktop or application window.
- **Media Engine:** The media processing tasks (encoding/decoding audio and video) are offloaded to the user's local device. This minimizes server load and optimizes network usage.

Typically, Citrix offers UCSDK to technology vendors in the real-time communications space and works with them to get UCSDK integrated into those applications. Once integrated, any Citrix customer using a UCSDK optimized application will have an enhanced experience. Citrix UCSDK can also be consumed by Citrix customers in cases where a custom in-house application is being built. In most cases, however, customers do not need to consume & develop with UCSDK – they just need to configure the Citrix environment and the application to achieve an optimized experience.

NOTE:

References of Citrix WebRTC SDK (or) an HDX™ optimized application indicate integration with Citrix UCSDK and can be used interchangeably.

What’s New

UCSDK 4.1.0 is the latest Generally available version that technology vendors can integrate. In addition, there are two more releases which are supported – UCSDK 4.0.2 and UCSDK 3.1.0. New features are introduced with UCSDK releases and technology vendors need to ensure to upgrade the SDK in order for customers to receive the features. This way, Citrix customers can just focus on upgrading Citrix components necessary to get new features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With the release of UCSDK 4.1.0, we are introducing critical user experience enhancements and brand-new features that will allow for deeper integration with partners' products and more value for our customers.

New Features

- **UCSDK Endpoint Screen Recording (Tech Preview):** Addressing a key gap in compliance recording, new UCSDK APIs can now capture content on the endpoint, even when applications are running within VDI. This feature, currently in preview for Windows endpoints, allows technology vendors to enhance their applications to support endpoint screen recording on Citrix. Note that this feature is focused on enhancing vendor applications and is different from Citrix Session recording.
- **Session Reconnect handling:** A critical enhancement to Bootstrap significantly improves the browser application experience, bringing it closer to that of Electron-based desktop applications. Browser-based applications using Bootstrap can now dynamically handle Citrix session disconnects, providing a seamless user experience for end-users.
- **Support for New methods:** Added support for restarting ICE gathering and support for `iceCandidatePoolSize` in `RTCConfiguration`.
- **Better Error handling and Compliance Improvements:** Improved compliance to WebRTC specification for `getUserMedia`. Improved `getStats()` for `CitrixPeerConnection`, `RtpSender`, and `RtpReceiver` to return empty report instead of void in error conditions.

Fully compatible versions for UCSDK 4.1.0 include:

- Citrix Virtual Apps and Desktops™ 2503
- Citrix Workspace™ App for Windows 2503
- Citrix Workspace App for Mac 2503
- Citrix Workspace App for Linux 2503
- The latest ChromeOS/HTML5 release.

NOTE:

Citrix customers can reach out to technology vendors to upgrade the SDK (or) add support to specific features in case there are use cases that can be achieved with the newly introduced features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Key Benefits

When you are using applications optimized with Citrix UCSDK, you can expect:

- Enhanced media processing performance by offloading processor-intensive media encoding/decoding from the Citrix Virtual Delivery Agent (VDA) to the client endpoint, increasing overall responsiveness for end users.
- Reduced CPU and bandwidth usage on Citrix VDA, allowing IT to support more concurrent users per host and enterprises to scale Citrix virtual desktop deployments cost-effectively.
- Lower total cost of ownership for enterprises, as optimized endpoints extend legacy virtual desktop lifespans and reduce host infrastructure needs, thus reducing capital expenditures and operating costs over time.
- Support for Windows, Mac, Linux, ChromeOS, and HTML5 endpoint platforms.

Use Cases

UCSDK is purpose-built to optimize real-time communication applications that adhere to the WebRTC standard. Here are key scenarios and the types of WebRTC-based applications that can / already use UCSDK.

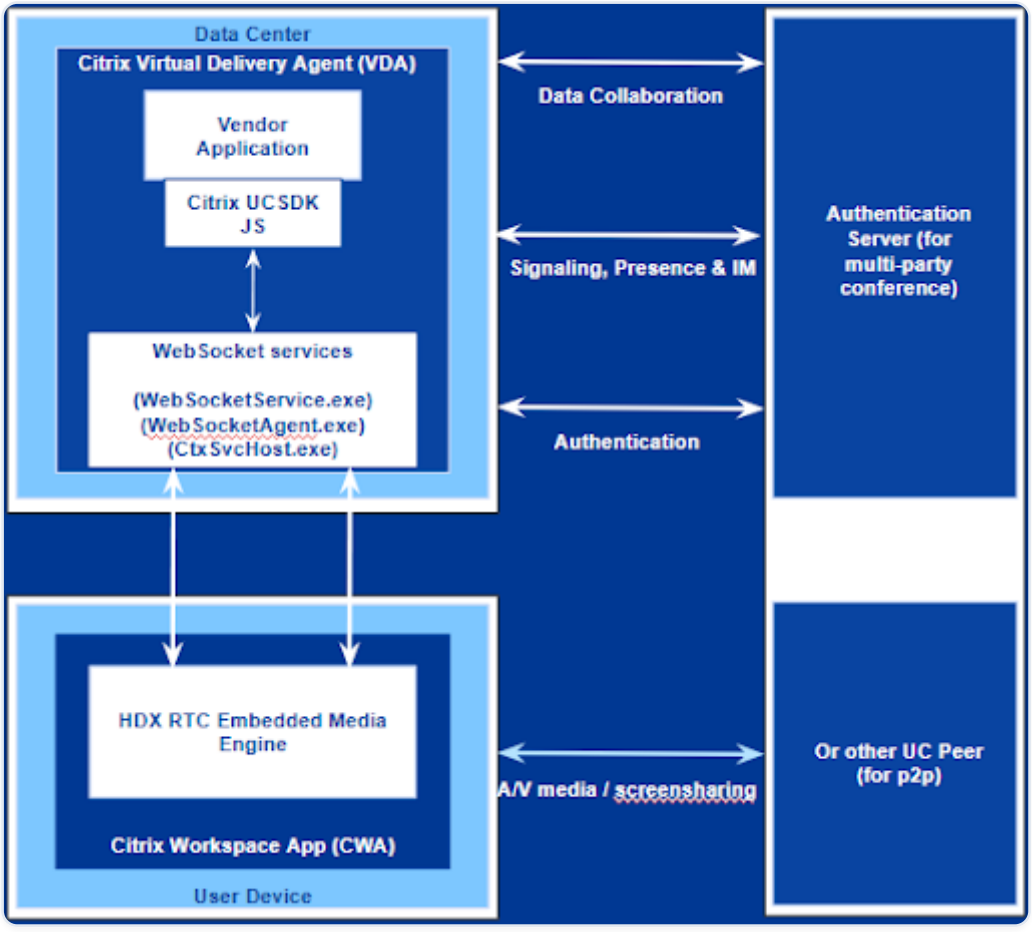
- **Contact Center as a Service (CCaaS) / Cloud Contact Center Platforms:** Primarily manage customer interactions across multiple channels, optimizing agent workflows.
    - Examples: Amazon Connect, Twilio, Avaya Experience Platform, Talkdesk, Content Guru
- **Unified Communications as a Service (UCaaS) / Cloud Business Communications:** Integrate voice, video, team messaging, and presence for comprehensive business communication.
    - Examples: Ring Central, 8x8, Intermedia, Alcatel-Lucent Rainbow
- **Communications Platform as a Service (CPaaS):** Provide APIs for embedding real-time communication capabilities directly into custom applications.
    - Examples: Twilio, Ribbon Communications
- **Enterprise Video Conferencing and Collaboration:** Dedicated platforms for high-quality video meetings, conferencing, and advanced collaboration features.
    - Example: Pexip

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Financial Trading Communications:** Engineered for the unique, high-performance, and compliant communication needs of financial markets.
  - Example: IPC Unigy
- **Virtual Learning and Training Platforms:** Designed for interactive, high-quality virtual classroom and training experiences.
  - Example: Vitero

The underlying WebRTC foundation of the Citrix UCSDK means its optimization capabilities can extend to any WebRTC-based communication applications. This opens the door for optimizing a wide array of applications that utilize WebRTC for real-time interactions, even if they are not currently listed as optimized with UCSDK. We encourage customers to reach out to Citrix with any use cases or applications they want to see optimized.

UCSDK Architecture



- Vendor application: This can be any third-party real-time communication application which is desktop-based or browser-based that integrated UCSDK.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- UCSDK JS: UCSDK JS provides the APIs that vendor applications utilize to offload the audio/video to the endpoint.
- HdxRtcEngine: This is the embedded WebRTC media engine in Citrix Workspace App that processes and handles the offloaded audio/video call.

Once the SDK is loaded and used, the `HdxRtcEngine.exe` process is launched on the client endpoint if redirection succeeds. Once `HdxRtcEngine.exe` is launched on the client endpoint, any signaling and payload data flows from Citrix VDA to the client endpoint, reaches the cloud, bounces back to the client endpoint, and then is forwarded to VDA. For example, a complete round trip of flow could be:

```
Vendor App -> CitrxWebrtc.js SDK -> Citrix VDA components -> Citrix Client Endpoint components -> Cloud -> Citrix Client Endpoint components -> Citrix VDA components -> CitrxWebrtc.js SDK -> Vendor App
```

System Requirements

The system requirements indicate the various versions of Citrix components needed with the latest version of UCSDK - 4.1.0. For compatibility details for older versions of the SDK and specific feature requirements, see Versions and Feature Matrix table below.

NOTE:

For customers to use any feature that is added to UCSDK – ensure that the vendor application has integrated the appropriate UCSDK version and enabled the feature and use the appropriate VDA and CWA versions in your environment.

Fully Compatible Versions

Fully compatible versions indicate that by using these versions of Citrix components along with the latest version of UCSDK, customers can take advantage of all the features available. For the current latest version of UCSDK – 4.1.0, fully compatible versions of Citrix components are as below:

- **Citrix Virtual Apps and Desktops:** 2503
- **Citrix Workspace App Windows:** 2503
- **Citrix Workspace App Mac:** 2503
- **Citrix Workspace App Linux:** 2503

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Citrix Workspace App ChromeOS/HTML5:** Latest version

Configuration

UCSDK feature functionality depends on three factors: the UCSDK version that the vendor has integrated and features that vendor has enabled, the Citrix Virtual Apps and Desktops, and the Citrix Workspace app version in use.

On the Citrix Side, please ensure the following is configured so that the optimized application is allowed to be optimized:

1. Ensure the Microsoft Teams redirection policy is turned on. Refer to Multimedia Policy Settings for more information. Note that this policy is ON by default.
2. Third-party Electron or browser-based applications that utilize the `CitrixWebrtc.js` SDK are not supported by default. The `CtxHdxWebSocketService` (`WebSocketService.exe`) will not allow connections from applications that are not on the allowlist. The desired application binary executable name must be added to a whitelist registry key.

On the VDA

- Create a Key Path: `HKLM\Software\WOW6432Node\Citrix\WebSocketService`
- KeyName: `ProcessWhitelist`
- Type: `MULTISZ`
- Key Value: `Mytestapp.exe`

If you have multiple applications, type each application in a new line. Do not copy and paste from a text file or insert commas. Make sure the name provided matches the executable name of the application. This registry value is not case-sensitive.

If the application is accessed through a browser instead of a full-fledged desktop application, then you need to allow for, e.g., `chrome.exe` in the registry value.

Once the above registry is configured successfully, reboot the VDA or restart `CtxHdxWebSocketService` to finish the Whitelist setup.

On the Client

No configuration is needed. Just install the Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Each vendor might have a very specific application name. Hence, refer to the vendor documentation linked in the Current Vendor Support section to determine which application name must be allowed in the WebSocketService.

Versions and Feature Matrix

As version updates happen frequently, please refer to Citrix Virtual Apps and Desktops and Citrix Workspace app product lifecycle pages to ensure a particular version is supported. For many of the older features, the versions mentioned in the table are the last supported Current Release (CR) versions at the time of writing this document.

FEATURE	UCSDK VERSION	VDA	CWA WINDOWS	CWA MAC	CWA LINUX	CWA CHROME OS/ HTML5
Audio / Video (p2p & conference)	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Screen sharing	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
DTMF	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Proxy Server Support	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
App Sharing	3.1.0	2203 LTSR Latest	2402 LTSR Latest	2311	2311	N/A

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	UCSDK VERSION	VDA	CWA WINDOWS	CWA MAC	CWA LINUX	CWA CHROME OS/ HTML5
		CU / 2311 CR	CU / 2311 CR			
Dynamic e911	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Multi Window	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
SDP Unified Plan Support	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Stream resolution / Simulcast	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Remote Audio (with Loop)	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2405
Browser-based UCSDK (Bootstrap support)	4.0.2	2407 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	UCSDK VERSION	VDA	CWA WINDOWS	CWA MAC	CWA LINUX	CWA CHROME OS/ HTML5
Web HID API	4.0.2	2203 LTSR Latest CU / 2311 CR	2409.10	2411	2411	2505
Web Audio API	4.0.2	2203 LTSR Latest CU / 2311 CR	2405	2405	2405	N/A
Restart ICE	4.1.0	2203 LTSR Latest CU / 2311 CR	2503.2	2503	2503	2502.10
Screen Recording (Preview) [1]	4.1.0	2503	2503.2	N/A	N/A	N/A

NOTE:

We've introduced a new policy for screen recording, so you need the 2503 version of the delivery controller™, which comes with CVAD 2503.

Current Vendor Support

Several third-party vendors have integrated the Unified Communications SDK into their products. The current list of vendors and their supporting documentation is listed below:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VENDOR	DOCUMENTATION
Amazon Connect	Optimize Amazon Connect audio for Citrix cloud desktops
Ring Central	Using RingCentral in a Citrix VDI environment
Five9	Five9 WebRTC in Citrix Environments
Twilio	Twilio Flex on Citrix VDI
Avaya	Avaya Experience Platform Public Cloud VDI solution for Citrix
8x8	Citrix VDI Integration with 8x8 Work for Desktop & Web
Content Guru	Content Guru Citrix Integration
Ribbon Communications	Ribbon Communications Citrix WebRTC SDK
Intermedia	Installing Intermedia Unite on Citrix Virtual Apps and Desktops
Alcatel-Lucent Rainbow	Citrix Optimization for Rainbow Desktop Application
Talkdesk	Talkdesk Agent Workspace VDI Connect
IPC	IPC Unigy Soft Client Citrix VDI
Vitero	Vitero Inspire for Citrix VDI
Pexip	Deploying Connect desktop app in Citrix Pexip Infinity Docs

Troubleshooting

For troubleshooting information, see Troubleshooting Guidance for Apps Optimized with Citrix Unified Communications SDK.

Known Issues & Limitations

This section will document the current known issues and limitations as they are recognized.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

General content redirection

Content redirection allows you to control whether users access information by using applications published on servers or by using applications running locally on user devices.

Client folder redirection

Client folder redirection changes the way client-side files are accessible on the host-side session.

- When you enable only client drive mapping on the server, client-side full volumes are automatically mapped to the sessions as Universal Naming Convention (UNC) links.
- When you enable client folder redirection on the server and the user configures it on the Windows desktop device, the portion of the local volume specified by the user is redirected.

Host to client redirection

Consider using host to client redirection for specific uncommon use cases. Normally, other forms of content redirection might be better. We support this type of redirection only on Multi-session OS VDAs and not on Single-session OS VDAs.

Local App Access and URL redirection

Local App Access seamlessly integrates locally installed Windows applications in to a hosted desktop environment. It does so without changing from one computer to another.

HDX™ technology provides **generic USB redirection** for specialty devices that don't have any optimized support or where it is unsuitable.

Client folder redirection

Client folder redirection changes the way client-side files are accessible on the host-side session. If you enable only client drive mapping on the server, client-side full volumes are automatically mapped as Universal Naming Convention (UNC) links to the sessions. When you enable client folder redirection on the server and the user configures it on the user device, the portion of the local volume specified by the user is redirected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Only the user-specified folders appear as UNC links inside sessions. That is, instead of the complete file system on the user device. If you disable UNC links through the registry, client folders appear as mapped drives inside the session.

Client folder redirection is supported on Windows Single-session OS machines only.

Client folder redirection for an external USB drive is not saved on detaching and reattaching the device.

Enable client folder direction on the server. Then, on the client device, specify which folders to redirect. The application you use to specify the client folder options is included with the Citrix Workspace™ app supplied with this release.

Requirements:

For servers:

- Windows Server 2019, Standard and Datacenter Editions
- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions

For clients:

- Windows 10, 32-bit and 64-bit editions (minimum version 1607)
- Windows 8.1, 32-bit and 64-bit editions (including Embedded edition)
- Windows 7, 32-bit and 64-bit editions (including Embedded edition)

To enable client folder redirection on the server, see Client folder redirection in the list of features managed through the registry.

On the user device, specify which folders to redirect:

1. Ensure that the latest version of Citrix Workspace app is installed.
2. From the Citrix Workspace app installation directory, start CtxCFRUI.exe.
3. Choose the **Custom** radio button and add, edit, or remove folders.
4. Disconnect and reconnect your sessions for the setting to take effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bidirectional content redirection configuration

Bidirectional content redirection allows URLs to be redirected from client to server or server to client, depending on the configurations. This policy setting replaces the following three settings, which are deprecated:

- Allow bidirectional content redirection
- Allowed URLs to be redirected to VDA
- Allowed URLs to be redirected to Client

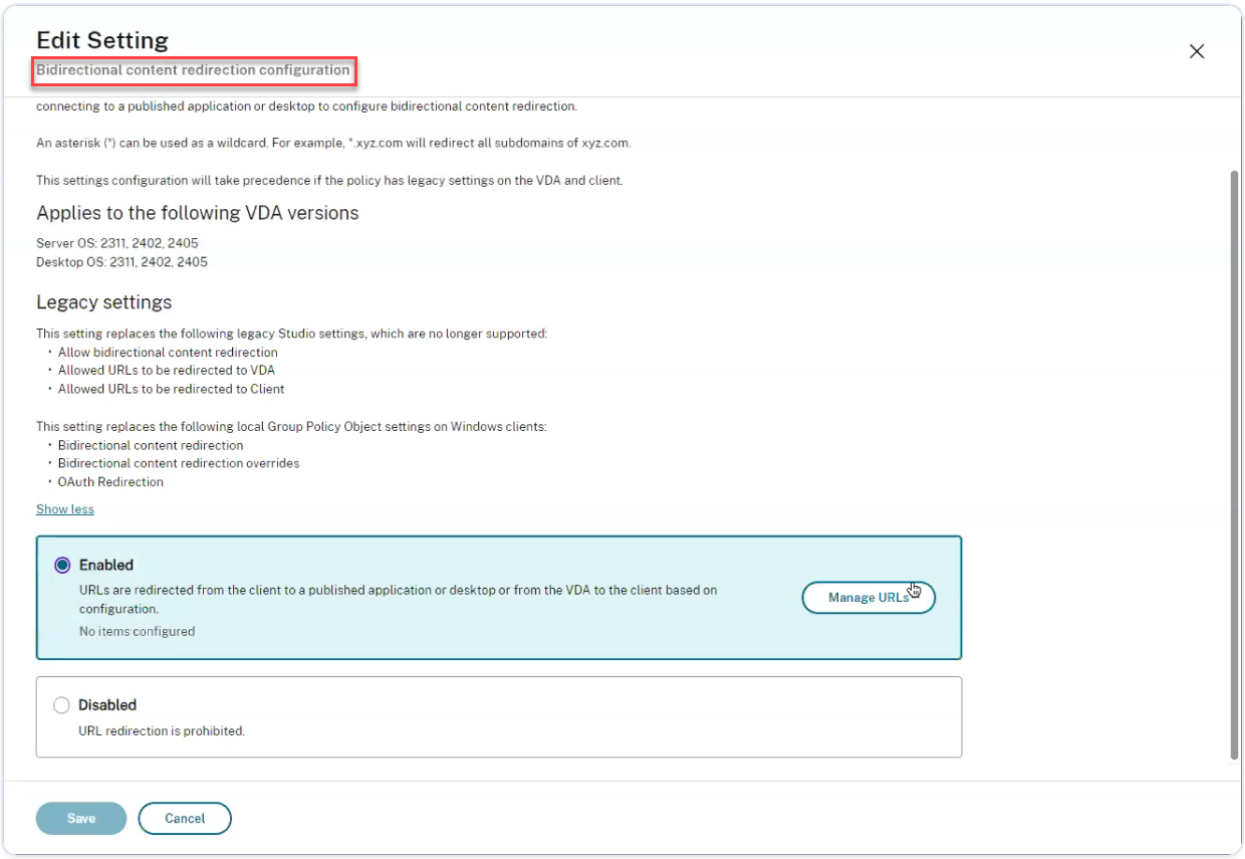
It also replaces the following three local GPO settings on Windows clients:

- Bidirectional content redirection
- Bidirectional content redirection overrides
- OAuth redirection

If this setting is configured, it takes precedence over the legacy settings in Studio and on the client. To configure the Bidirectional content redirection policy, do the following:

1. From Studio, select the **Policies node** and click the **Policies** tab.
2. Click **Create Policy**. The **Create Policy** blade opens.
3. Search for `Bidirectional content redirection configuration` in the **Search** field, select the check box and click **Edit**.
4. In the **Edit Setting** blade, set this policy to **Enabled** and click **Manage URLs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. In the **Manage URLs** blade, for **VDA-to-client redirection** specify the following:

   - **URL** (Required): Add the URL that should redirect from the VDA to open on the client. For OAuth redirection, set the authentication scheme and pattern on the client to redirect the session back to the host.
   - **Pattern** (Optional): URL regular expression that, when redirected to the client through VDA-to-Client URL redirection, is tracked as if an OAuth authentication flow has begun, and when the flow completes (detected by the resulting scheme or redirect URL pattern being opened), that resulting URL is redirected back into the Host VDA that initiated that flow.
   - **Scheme** (Optional): If a Scheme is specified, the terminating URL is expected to be of the form: `scheme://<something>`. If Scheme is not specified (empty), then the original resulting URL pattern is extracted from the Pattern via a regular expression capture group (must be specified in the Pattern), and the original URL is rewritten to use a `citrix-oauth-redir://` redirect URL. When the flow completes, the original redirect URL is then redirected back into the Host (VDA). Any OAuth Authorization server, in this case, must be configured to allow `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` redirect URLs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Though both **Pattern** and **Scheme** are optional, if **Pattern** is specified, you must also specify **Scheme**.

6. In the **Manage URLs** blade, for **Client-to-VDA redirection** specify the following:
   - **Type**: Choose **Desktop** or **Application**.
   - **Name**: Provide a name to the type.
   - **URL**: Provide the URL you want to redirect to the source. You can add multiple URLs and delete the ones that are not required
7. Click **Save**. The **Edit Setting** blade displays the number of items configured.
8. Click **Save**. The **Create Policy** blade displays the **Current Value** configured. Click **Next**.
9. In the **Assign Policy To** step, click **Next**.
10. In the **Summary** step, select the **Enable policy** check box and provide a name in the **Policy name** field.
11. Click **Finish**. The new policy is listed.
12. Select the new policy created to review the settings configured.

For legacy settings see Host-to-client redirection and Bidirectional content redirection.

Host-to-client redirection

NOTE:

This article describes the legacy host-to-client redirection settings. For the latest settings, see Bidirectional content redirection configuration. The new policy settings will take precedence over the legacy settings. Citrix recommends using only the new policy settings and deleting any legacy settings to avoid unexpected behavior.

Host-to-client redirection allows URLs, embedded as hyperlinks in applications running on a Citrix® session, to open using the corresponding application on the user endpoint device. Some common use cases for host-to-client redirection include:

- Redirection of websites in cases where the Citrix server doesn't have Internet or network access to the source.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Redirection of websites when running a web browser inside the Citrix session is not desired for security, performance, compatibility, or scalability reasons.
- Redirection of specific URL types in cases where the required applications to open the URL are not installed on the Citrix server.

Host-to-client redirection is not intended for URLs that you access on a webpage or type in the address bar of the web browser running in the Citrix session. For redirection of URLs in web browsers, see Bidirectional URL redirection or Browser content redirection.

System requirements

- Multi-session OS VDA
- Supported clients:
  - Citrix Workspace™ app for Windows
  - Citrix Workspace app for Mac
  - Citrix Workspace app for Linux
  - Citrix Workspace app for HTML5
  - Citrix Workspace app for Chrome

The client device must have an application installed and configured for handling the redirection of the URL types.

Configuration

Use the Host-to-client redirection Citrix policy to enable this functionality. **Host to client redirection** is disabled by default. After you enable the Host-to-client redirection policy, the Citrix Launcher application registers with the Windows server to ensure that it can intercept URLs and send them to the client device.

Then you must configure the Windows Group Policy to use Citrix Launcher as the default application for the required URL types. On the Citrix server VDA, create the ServerFTAdefaultPolicy.xml file and insert the following XML code.

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

From the Group Policy management console, go to **Computer configuration > Administrative Templates > Windows Components > File Explorer > Set a default associations configuration file**, and save your ServerFTAdefaultPolicy.xml file.

NOTE:

If a Citrix server doesn't have the Group Policy settings, Windows prompts users to select an application for opening URLs.

By default, we support redirection of the following URL types:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

To include additional standard or custom URL types on the list for redirection, create a new **Association Identifier** line in the ServerFTAdefaultPolicy.xml file referenced earlier. For example:

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

Adding URL types to the list also requires client configuration. Create the following registry key and values on the Windows client.

NOTE:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Value name: ExtraURLProtocols
- Value type: REG_SZ
- Value data: Specify the required URL types separated by semicolon. Include everything before the authority portion of the URL. For example:
  `ftp://;mailto:;customtype1://;custometype2://`

You can add URL types only for Windows clients. Clients missing the registry settings above reject redirection back to the Citrix session. Client must have an application installed and configured to handle the specified URL types.

To remove URL types from the default redirection list, create the following registry key and values on the server VDA.

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Value name: DisableServerFTA
- Value type: DWORD
- Value data: 1
- Value name: NoRedirectClasses
- Value type: REG_MULTI_SZ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Value data: Specify any combination of the values: `http`, `https`, `rtsp`, `rtspu`, `pnm`, or `mms`. Type multiple values on separate lines. For example:

```
http
```

```
https
```

```
rtsp
```

To enable host-to-client redirection for a specific set of websites, create a registry key and values on the server VDA.

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Value name: ValidSites
- Value type: REG_MULTI_SZ
- Value data: Specify any combination of fully qualified domain names (FQDNs). Type multiple FQDNs on separate lines. Include the FQDN only, without protocols (`http://` or `https://`). An FQDN can include an asterisk (`*`) as a wildcard character in the leftmost position only. This wildcard matches a single level of domain, which is consistent with the rules in RFC 6125. For example:

```
www.exmaple.com
```

```
*.example.com
```

NOTE:

You cannot use the **ValidSites** key in combination with the **DisableServerFTA** and **NoRedirectClasses** keys.

Server VDA default browser configuration

Enabling host-to-client redirection as referenced in this section supersedes any previous default browser configuration on the server VDA. If a web URL is not redirected, the Citrix Launcher passes the URL to the browser configured in the `command_backup` registry key. The key points to Internet Explorer by default, but you can modify it to include the path to a different browser. For more information, see Server VDA default browser configuration in the list of features managed through the registry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bidirectional content redirection

NOTE:

This article describes the legacy bidirectional content redirection settings. For the latest policy settings, see Bidirectional content redirection configuration. The new policy settings will take precedence over the legacy settings. Citrix recommends using only the new policy settings and deleting any legacy settings to avoid unexpected behavior.

Bidirectional content redirection allows HTTP or HTTPS URLs in web browsers, or embedded into applications, to be forwarded between the Citrix VDA session and the client endpoint in both directions. A URL entered in a browser running in the Citrix session can be opened using the client's default browser. Conversely, a URL entered in a browser running on the client can be opened in a Citrix session, either with a published application or desktop. Some common use cases for bidirectional content redirection include:

- Redirection of web URLs in cases where the starting browser does not have network access to the source.
- Redirection of web URLs for browser compatibility and security reasons.
- Redirection of web URLs embedded in applications when running a web browser on the Citrix session or the client isn't wanted.

System requirements

- Single-session or multi-session OS VDAs
- Citrix Workspace™ app for Windows

Browsers:

- Google Chrome with Citrix Browser Redirection Extension (available on the Google Chrome Web Store)
- Microsoft Edge (Chromium) with Citrix Browser Redirection Extension (available on the Google Chrome Web Store)

Configuration

Bidirectional content redirection must be enabled using the Citrix policy on both the VDA and client for redirection to work. Bidirectional content redirection is disabled by default.

For VDA configuration, see Bidirectional content redirection in the ICA policy settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For client configuration, see Bidirectional content redirection in the Citrix Workspace app for Windows documentation.

Browser extensions must be registered using the commands shown. Run the commands as needed on the VDA and client based on the browser in use.

To register the browser extensions on the VDA, open a command prompt. Then, run `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` with the required browser option as shown in the examples shown:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

To register the extension on all available browsers run:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

To unregister a browser extension use the `/unreg<browser>` option as in the example shown:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

To register the browser extensions on the client open a command prompt and run `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` with the same options as the examples shown.

NOTE:

The register command causes Chrome and Edge browsers to prompt users to enable the Citrix Browser Redirection Extension during first launch. The browser extension can also be installed manually from the Google Chrome Web Store.

Wildcard redirection from Citrix VDA to client

Bidirectional content redirection supports the use of wildcards when defining the URLs to be redirected. To configure bidirectional content redirection, see the configuration instructions.

In Citrix Studio, set the wildcard URL in **Allowed URLs to be redirected to Client**. The asterisk (*) is the wildcard character.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Don't set the **Allowed URLs to be redirected to VDA** in the client policy. Ensure that the sites set the **Allowed URLs to be redirected to VDA** to avoid infinite redirection loops.
- Top-level domains are not supported. For example, `https://www.citrix.*` or `http://www.citrix.co*` is not redirected.

Custom protocol redirection from VDA to client

Bidirectional content redirection supports redirecting custom protocols from the Citrix VDA to the client. Protocols other than HTTP or HTTPS are supported. To configure bidirectional content redirection, see the configuration instructions.

In Citrix Studio, set the custom protocol in **Allowed URLs to be redirected to Client**.

NOTE:

- The client must have an application registered to handle the protocol. Otherwise, the URL redirects to the client and fails to launch.
- Custom protocol URLs that you enter or launch in the Chrome and Edge browsers are not supported and not redirected.
- The following protocols are not supported: `rtsp://, rtspu://, pnm://, mms://`.

Other considerations

- Browser requirements and configurations are only applicable to the browser starting the redirection. The destination browser, where the URL opens after redirection is successful, isn't considered for support. When redirecting URLs from the VDA to a client, a supported browser configuration is only required on the VDA. Conversely, when redirecting URLs from the client to a VDA, a supported browser configuration is only required on the client. Redirected URLs are handed off to the default browser configured on the destination machine, either the client or the VDA, depending on direction. Using the same browser type on the VDA and the client is NOT required.
- Check that redirection rules do not result in a looping configuration. For example, a VDA policy is set to redirect `https://www.citrix.com`, and the client policy is set to redirect the same URL, resulting in infinite looping.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Only HTTP/HTTPS protocol URLs are supported. URL shorteners aren't supported.
- Client to VDA redirection requires the Windows client to be installed with administrator rights.
- If the destination browser is already open, the redirected URL opens in a new tab. Otherwise the URL opens in a new browser window.
- Bidirectional content redirection does not work when Local App Access (LAA) is enabled.

Local app access and URL redirection

Introduction

Local App Access seamlessly integrates locally installed Windows applications into a hosted desktop environment without switching from one desktop to another. With Local App Access, you can:

- Access applications installed locally on a physical laptop, PC, or other device directly from the virtual desktop.
- Provide a flexible application delivery solution. If users have local applications that you cannot virtualize or that IT does not maintain, those applications still behave as though they are installed on a virtual desktop.
- Eliminate the double-hop latency when applications are hosted separately from the virtual desktop. Do so by putting a shortcut to the published application on the user's Windows device.
- Use applications such as:
  - Video conferencing software such as GoToMeeting.
  - Specialty or niche applications that are not yet virtualized.
  - Applications and peripherals that would otherwise transfer large amounts of data from a user device to a server and back to the user device. For example, DVD burners and TV tuners.

In Citrix Virtual Apps and Desktops™, hosted desktop sessions use URL redirection to start Local App Access applications. URL redirection makes the application available under more than one URL address. It launches a local browser (based on the browser's URL block list) by selecting embedded links within a browser in a desktop session. If you navigate to a URL that is not present in the block list, the URL is opened in the desktop session again.

URL redirection works only for desktop sessions, not application sessions. The only redirection feature you can use for application sessions is host-to-client content redirection, which is a type of

© 1997–2026 Citrix Systems, Inc. All rights reserved.

server FTA (File Type Association) redirection. This FTA redirects certain protocols to the client, such as HTTP, HTTPS, RTSP, or MMS. For example, if you only open embedded links with HTTP, the links directly open with the client application. There is no URL block list or allow list support.

When Local App Access is enabled, URLs that are displayed to users as links from locally running applications, from user-hosted applications, or as shortcuts on the desktop are redirected in one of the following ways:

- From the user's computer to the hosted desktop
- From the Citrix Virtual Apps and Desktops server to the user's computer
- Rendered in the environment in which they are started (not redirected)

To specify the redirection path of content from specific websites, configure the URL allow list and URL block list on the Virtual Delivery Agent. Those lists contain multi-string registry keys that specify the URL redirection policy settings. For more information, see the Local App Access policy settings.

URLs can be rendered on the VDA with the following exceptions:

- Geo/Locale information — Websites that require locale information, such as msn.com or news.google.com (opens a country specific page based on the Geo). For example, if the VDA is provisioned from a data center in the UK and the client is connecting from India, the user expects to see in.msn.com. Instead, the user sees uk.msn.com.
- Multimedia content — Websites containing rich media content, when rendered on the client device, give the end users a native experience and also save bandwidth even in high latency networks. This feature redirects sites with other media types such as Silverlight. This process is in a secure environment. That is, the URLs that the administrator approves are run on the client while the rest of the URLs are redirected to the VDA.

In addition to URL redirection, you can use FTA redirection. FTA starts local applications when a file is encountered in the session. If the local app is started, the local app must have access to the file to open it. Therefore, you can only open files that reside on network shares or on client drives (using client drive mapping) using local applications. For example, when opening a PDF file, if a PDF reader is a local app, then the file opens using that PDF reader. Because the local app can access the file directly, there is no network transfer of the file through ICA® to open the file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements, considerations, and limitations

We support Local App Access on the valid operating systems for VDAs for Windows Multi-session OS and for VDAs for Windows Single-session OS. Local App Access requires Citrix Workspace app for Windows version 4.1 (minimum). The following browsers are supported:

- Edge, latest version
- Firefox, latest version and extended support release
- Chrome, latest version

Review the following considerations and limitations when using Local App Access and URL redirection.

- Local App Access is designed for full-screen, virtual desktops spanning all monitors:
  - The user experience can be confusing if you use Local App Access with a virtual desktop that runs in windowed mode or does not cover all monitors.
  - Multiple monitors — When one monitor is maximized, it becomes the default desktop for all applications started in that session. This default occurs even if the subsequent applications typically start on another monitor.
  - The feature supports one VDA. There is no integration with multiple concurrent VDAs.
- Some applications can behave unexpectedly, affecting users:
  - The drive letters might confuse users, such as local C: rather than virtual desktop C: drive.
  - Available printers in the virtual desktop are not available to local applications.
  - Applications that require elevated permissions cannot be started as client-hosted applications.
  - There is no special handling for single-instance applications (such as Windows Media Player).
  - Local applications appear with the Windows theme of the local machine.
  - Full-screen applications are not supported. These applications include applications that open to a full screen, such as PowerPoint slide shows or photo viewers that cover the entire desktop.
  - Local App Access copies the properties of the local application (such as the shortcuts on the client's desktop and Start menu) on the VDA. However, it does not copy other properties such as shortcut keys and read-only attributes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Applications that customize how overlapping window order is handled can have unpredictable results. For example, some windows might be hidden.
    - Shortcuts are not supported, including My Computer, Recycle Bin, Control Panel, Network Drive shortcuts, and folder shortcuts.
    - The following file types and files are not supported: custom file types, files with no associated programs, zip files, and hidden files.
    - Taskbar grouping is not supported for mixed 32-bit and 64-bit client-hosted or VDA applications. That is, grouping 32-bit local applications with 64-bit VDA applications.
    - Applications cannot be started using COM. For example, if you click an embedded Office document from within an Office application, the process start cannot be detected, and the local application integration fails.

- Double-hop scenarios, where a user is starting a virtual desktop from within another virtual desktop session, are not supported.
- URL redirection supports only explicit URLs (that is, URLs appearing in the browser's address bar or found using the in-browser navigation, depending on the browser).
- URL redirection works only with desktop sessions, not with application sessions.
- The local desktop folder in a VDA session does not allow users to create files.
- Multiple instances of a locally running application behave according to the taskbar settings established for the virtual desktop. However, shortcuts to locally running applications are not grouped with running instances of those applications. They are also not grouped with running instances of hosted applications or pinned shortcuts to hosted applications. Users can close only windows of locally running applications from the Taskbar. Although users can pin local application windows to the desktop Taskbar and Start menu, the applications might not start consistently when using these shortcuts.
- If you set the **Allow local app access** policy setting to **Enabled**, browser content redirection isn't supported.

Interaction with Windows

The Local App Access interaction with Windows includes the following behaviors.

- Windows 8 and Windows Server 2012 shortcut behavior
    - Windows Store applications installed on the client are not enumerated as part of Local App Access shortcuts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - Image and video files are opened by default using Windows store applications. However, Local App Access enumerates the Windows store applications and opens shortcuts with desktop applications.

- Local Programs
  - For Windows 7, the folder is available in the Start menu.
  - For Windows 8, Local Programs is available only when the user chooses **All Apps** as a category from the Start screen. Not all subfolders are displayed in Local Programs.
- Windows 8 graphics features for applications
  - Desktop applications are restricted to the desktop area and are covered by the Start screen and Windows 8 style applications.
  - Local App Access applications do not behave like desktop applications in multi-monitor mode. In multi-monitor mode, the Start screen and the desktop display on different monitors.
- Windows 8 and Local App Access URL Redirection
  - Because Windows 8 Internet Explorer has no add-ons enabled, use desktop Internet Explorer to enable URL redirection.
  - In Windows Server 2012, Internet Explorer disables add-ons by default. To implement URL Redirection, disable the Internet Explorer enhanced configuration. Then reset the Internet Explorer options and restart to ensure that add-ons are enabled for standard users.

Configure Local App Access and URL redirection

To use Local App Access and URL redirection with Citrix Workspace™ app:

- Install Citrix Workspace app on the local client machine. You can enable both features during the Citrix Workspace app installation or you can enable Local App Access template using the Group Policy editor.
- Set the **Allow local app access** policy setting to **Enabled**. You can also configure URL allow list and block list policy settings for URL redirection. For more information, see Local App Access policy settings.

Enable Local App Access and URL redirection

To enable Local App Access for all local applications, follow these steps:

1. From Studio, select **Policies** in the left pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select **Create Policy** in the action bar.
3. In the Create Policy window, type “Allow Local App Access” in the search box and then click **Select**.
4. In the Edit Setting window, select **Allowed**. By default, the **Allow local app access** policy is prohibited. When this setting is allowed, the VDA allows the end-user to decide whether published applications and Local App Access shortcuts are enabled in the session. (When this setting is prohibited, both published applications and Local App Access shortcuts do not work for the VDA.) This policy setting applies to the entire machine and the URL redirection policy.
5. In the Create Policy window, type “URL redirection allow list” in the search box and then click **Select**. The URL redirection allow list specifies URLs to open in the default browser of the remote session.
6. In the Edit Setting window, click **Add** to add the URLs and then click **OK**.
7. In the Create Policy window, type “URL redirection block list” in the search box and then click **Select**. The URL redirection block list specifies URLs that are redirected to the default browser running on the endpoint.
8. In the Edit Setting window, click **Add** to add the URLs and then click **OK**.
9. On the Settings page, click **Next**.
10. On the Users and Machines page, assign the policy to the applicable Delivery Groups and then click **Next**.
11. On the Summary page, review the settings and then click **Finish**.

To enable URL redirection for all local applications during Citrix Workspace app installation, follow the steps below:

1. Enable URL redirection when you install Citrix Workspace app for all users on a machine. Doing so also registers the browser add-ons required for URL redirection.
2. From the command prompt, run the appropriate command to install the Citrix Workspace app using one of the following options:

    - For CitrixReceiver.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
    - For CitrixReceiverWeb.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable the Local App Access template using the Group Policy editor

NOTE:

- Before you enable the Local App Access template using the Group Policy editor, add the `receiver.admx/adml` template files to the local GPO. For more information, see Get started and search for *Group Policy Object administrative template*.
- Citrix Workspace app for Windows template files are available in the local GPO in **Administrative Templates > Citrix Components > Citrix Workspace** folder only when you add the `CitrixBase.admx/CitrixBse.adml` to the %systemroot% \policyDefinitions folder.

To enable the Local App Access template using the Group Policy editor, follow these steps:

1. Run **gpedit.msc**.
2. Go to **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Workspace > User Experience**.
3. Click **Local App Access settings**.
4. Select **Enabled** and then select **Allow URL Redirection**. For URL redirection, register browser add-ons using the command line described in the *Register browser add-ons* section further down in this article.

Provide access only to published applications

You can provide access to published applications using the Registry Editor or the PowerShell SDK.

To the Registry Editor, see The Local App Access for published applications in the list of features managed through the registry.

To use the PowerShell SDK:

1. Open PowerShell on the machine where the Delivery Controller™ is running.
2. Enter the following command: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`.

To have access to **Add Local App Access Application** in a Citrix DaaS deployment, use the Citrix Virtual Apps and Desktops Remote PowerShell SDK. For more information, see Citrix Virtual Apps and Desktops Remote PowerShell SDK.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Download the installer:

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`

2. Run these commands:

   a. `asnp citrix.*`

   b. `Get-XdAuthentication`

3. Enter the following command: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`.

After you complete the applicable preceding steps, follow these steps to continue.

1. From Studio, select **Applications** in the left pane.
2. In the upper middle pane, right-click the blank area and select **Add Local App Access Application** from the menu. You can also click **Add Local App Access Application** in the Actions pane. To display the Add Local App Access Application option in the Actions pane, click **Refresh**.
3. Publish Local App Access application.

   - The Local Application Access wizard launches with an Introduction page, which you can remove from future launches of the wizard.
   - The wizard guides you through the Groups, Location, Identification, Delivery, and Summary pages described below. When you are finished with each page, click **Next** until you reach the Summary page.
   - On the Groups page, select one or more Delivery Groups where the new applications will be added, and then click **Next**.
   - On the Location page, type the full executable path of the application on the user's local machine, and type the path to the folder where the application is located. Citrix recommends that you use the system environment variable path; for example, %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
   - On the Identification page, accept the default values or type the information that you want and then click **Next**.
   - On the Delivery page, configure how this application is delivered to users and then click **Next**. You can specify the icon for the selected application. You can also specify whether the shortcut to the local application on the virtual desktop will be visible on the Start menu, the desktop, or both.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On the Summary page, review the settings and then click **Finish** to exit the Local Application Access wizard.

Register browser add-ons

NOTE:

The browser add-ons required for URL redirection are registered automatically when you install Citrix Workspace app from the command line using the `/ALLOW_CLIENTHOSTEDAPPSURL=1` option.

You can use the following commands to register and unregister one or all add-ons:

- To register add-ons on a client device: \<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- To unregister add-ons on a client device: \<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- To register add-ons on a VDA: \<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- To unregister add-ons on a VDA: \<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

Where \<*browser*> is Internet Explorer, Firefox, Chrome, or All.

For example, the following command registers Internet Explorer add-ons on a device running Citrix Workspace app.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

The following command registers all add-ons on a Windows Multi-session OS VDA.

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

URL interception across browsers

- By default, Internet Explorer redirects the specified URL. If the URL is not in the block list but the browser or website redirects it to another URL, the final URL is not redirected. It is not redirected even if it is on the block list.

For URL redirection to work correctly, enable the add-on when prompted by the browser. If the add-ons that are using Internet options or the add-ons in the prompt are disabled, URL redirection does not work correctly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Firefox add-ons always redirect the URLs.

When an add-on is installed, Firefox prompts to allow or prevent installing the add-on on a new tab page. Allow the add-on for the feature to work.

- The Chrome add-on always redirects the final URL that is navigated, and not the entered URLs.

The extensions have been installed externally. When you disable the extension, the URL redirection feature does not work in Chrome. If the URL redirection is required in Incognito mode, allow the extension to run in that mode in the browser settings.

Configure local application behavior on logoff and disconnect

NOTE:

If you do not follow these steps to configure the settings, by default, local applications continue to run when a user logs off or disconnects from the virtual desktop. After reconnection, local applications are reintegrated if they are available on the virtual desktop.

To configure local application behavior on logoff and disconnect, see Local application behavior on logoff and disconnect in the list of features managed through the registry.

Generic USB redirection and client drive considerations

HDX™ technology provides **optimized support** for most popular USB devices. Optimized support offers an improved user experience with better performance and bandwidth efficiency over a WAN. Optimized support is usually the best option, especially in high latency or security-sensitive environments.

HDX technology provides **generic USB redirection** for specialty devices that don't have optimized support or where it is unsuitable, for example:

- The USB device has more advanced features that are not part of optimized support, such as a mouse or webcam having more buttons.
- Users need functions which are not part of optimized support.
- The USB device is a specialized device, such as test and measurement equipment or an industrial controller.
- An application requires direct access to the device as a USB device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The USB device only has a Windows driver available. For example, a smart card reader might not have a driver available for Citrix Workspace™ app for Android.
- The version of Citrix Workspace app does not provide any optimized support for this type of USB device.

With generic USB redirection:

- Users do not need to install device drivers on the user device.
- USB client drivers are installed on the VDA machine.

IMPORTANT:

- Generic USB redirection can be used together with optimized support. If you enable generic USB redirection, configure Citrix USB devices policy settings for both generic USB redirection and optimized support.
- The Citrix policy setting in Client USB device optimization rules is a specific setting for generic USB redirection, for a particular USB device. It doesn't apply to optimized support as described here.
- When brokering a session using Citrix® software to an Azure Virtual Machine, Citrix provides best effort support for USB redirection to the Azure Virtual Machine. We support fixing a Citrix software problem, but we do not support the underlying Azure Virtual Machine.
- CD/DVD devices with disc burning capabilities can be redirected, but the burning capabilities of these devices cannot be used. This is due to the buffer limits of a session.

Performance considerations for USB devices

Network latency and bandwidth can affect user experience and USB device operation when using generic USB redirection for some types of USB devices. For example, timing-sensitive devices might not operate correctly over high-latency low-bandwidth links. Use optimized support instead where possible.

Some USB devices require high bandwidth to be usable, for example a 3D mouse (used with 3D apps that also typically require high bandwidth). If bandwidth cannot be increased, you might be able to mitigate the issue by tuning bandwidth usage of other components using the bandwidth policy settings. For more information, see Bandwidth policy settings for Client USB device redirection, and Multi-stream connection policy settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security considerations for USB devices

Some USB devices are security-sensitive by nature, for example, smart card readers, fingerprint readers, and signature pads. Other USB devices such as USB storage devices can be used to transmit data that might be sensitive.

USB devices are often used to distribute malware. Configuration of Citrix Workspace app and Citrix Virtual Apps and Desktops™ can reduce, but not eliminate, risk from these USB devices. This situation applies whether generic USB redirection or optimized support is used.

IMPORTANT:

For security-sensitive devices and data, always secure the HDX connection using either TLS or IPsec.

Only enable support for the USB devices that you need. Configure both generic USB redirection and optimized support to meet this need.
Provide guidance to users for safe use of USB devices:

- Use only USB devices that have been obtained from a trustworthy source.
- Don't leave USB devices unattended in open environments - for example, a flash drive in an internet cafe.
- Explain the risks of using a USB device on more than one computer.

Compatibility with generic USB redirection

Generic USB redirection is supported for USB 2.0 and earlier devices. Generic USB redirection is also supported for USB 3.0 devices connected to a USB 2.0 or USB 3.0 port. Generic USB redirection does not support USB features introduced in USB 3.0, such as super speed.

These Citrix Workspace apps support generic USB redirection:

- Citrix Workspace app for Windows, see Configuring application delivery.
- Citrix Workspace app for Mac, see Citrix Workspace app for Mac.
- Citrix Workspace app for Linux, see Optimize.
- Citrix Workspace app for Chrome OS, see Citrix Workspace app for Chrome.

For Citrix Workspace app versions, see the Citrix Workspace app feature matrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you are using earlier versions of Citrix Workspace app, see the Citrix Workspace app documentation to confirm that generic USB redirection is supported. See Citrix Workspace app documentation for any restrictions on USB device types that are supported.

Generic USB redirection is supported for desktop sessions from VDA for Single-session OS version 7.6 through current.

Generic USB redirection is supported for desktop sessions from VDA for Multi-session OS version 7.6 through current, with these restrictions:

- The VDA must be running Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022.
- The USB device drivers must be fully compatible with Remote Desktop Session Host (RDSH) for the VDA OS (Windows 2012 R2), including full virtualization support.

Some types of USB devices are not supported for generic USB redirection because it would not be useful to redirect them:

- USB modems.
- USB network adapters.
- USB hubs. The USB devices connected to USB hubs are handled individually.
- USB virtual COM ports. Use COM port redirection rather than generic USB Redirection.

For information on USB devices that have been tested with generic USB redirection, see Citrix Ready Marketplace. Some USB devices do not operate correctly with generic USB redirection.

Configure generic USB redirection

You can control, and separately configure, which types of USB devices use generic USB redirection:

- On the VDA, using Citrix policy settings. For more information, see Redirection of client drives and user devices and USB devices policy settings in the Policy settings reference
- In Citrix Workspace app, using Citrix Workspace app-dependent mechanisms. For example, an Administrative Template controls registry settings that configure Citrix Workspace app for Windows. By default, USB redirection is allowed for certain classes of USB devices and denied for others. For more information, see Configure in the Citrix Workspace app for Windows documentation.

This separate configuration provides flexibility. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If two different organizations or departments are responsible for Citrix Workspace app and VDA, they can enforce control separately. This configuration applies when a user in one organization accesses an application in another organization.
- Citrix policy settings can control USB devices that are allowed only for certain users or for users connecting only over a LAN (rather than by using Citrix Gateway).

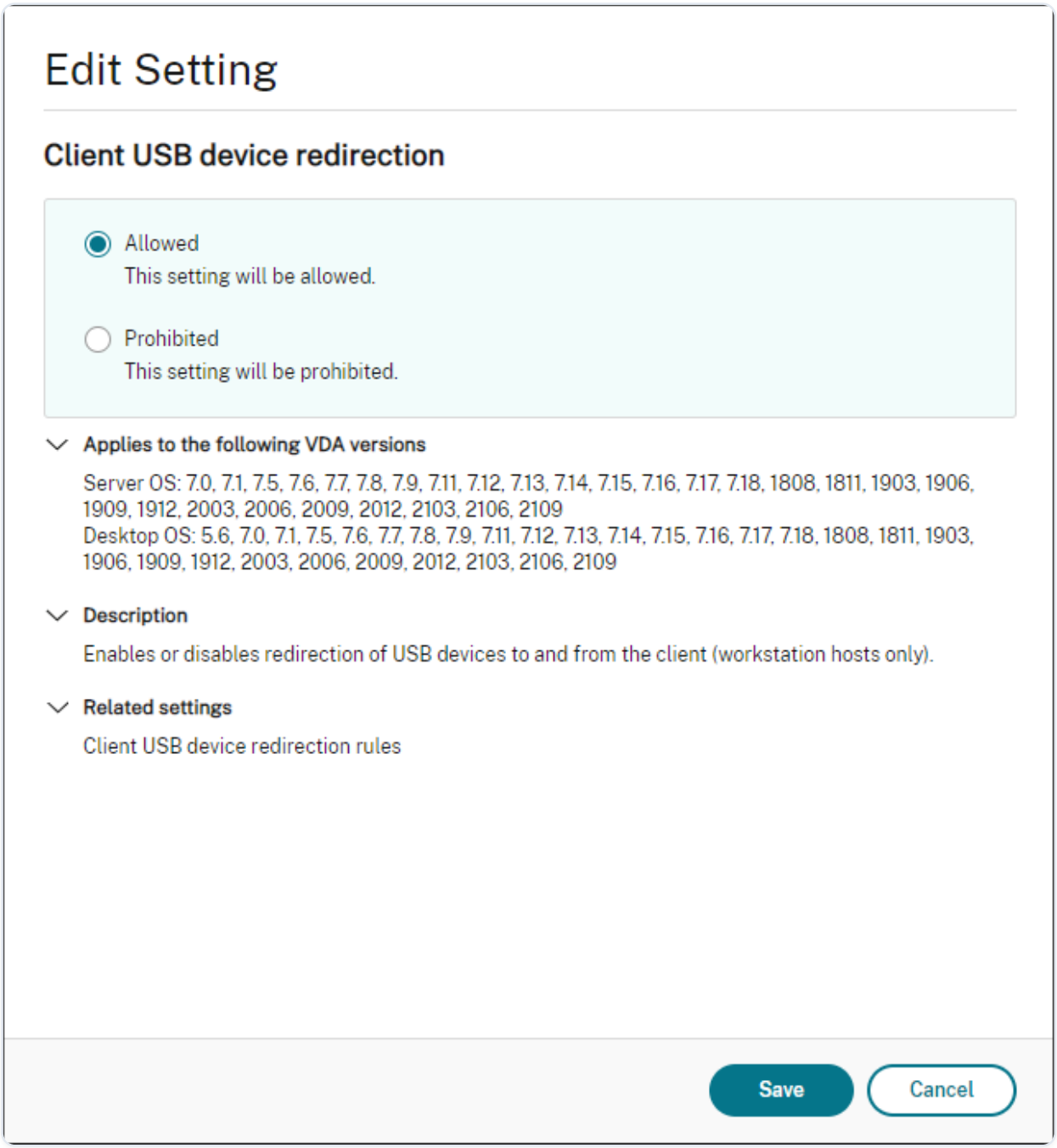
Enable generic USB redirection

To enable generic USB Redirection, and not require manual redirection by the user, configure both Citrix policy settings and Citrix Workspace app connections preferences.

In Citrix policy settings:

1. Add the Client USB device redirection to a policy and set its value to **Allowed**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

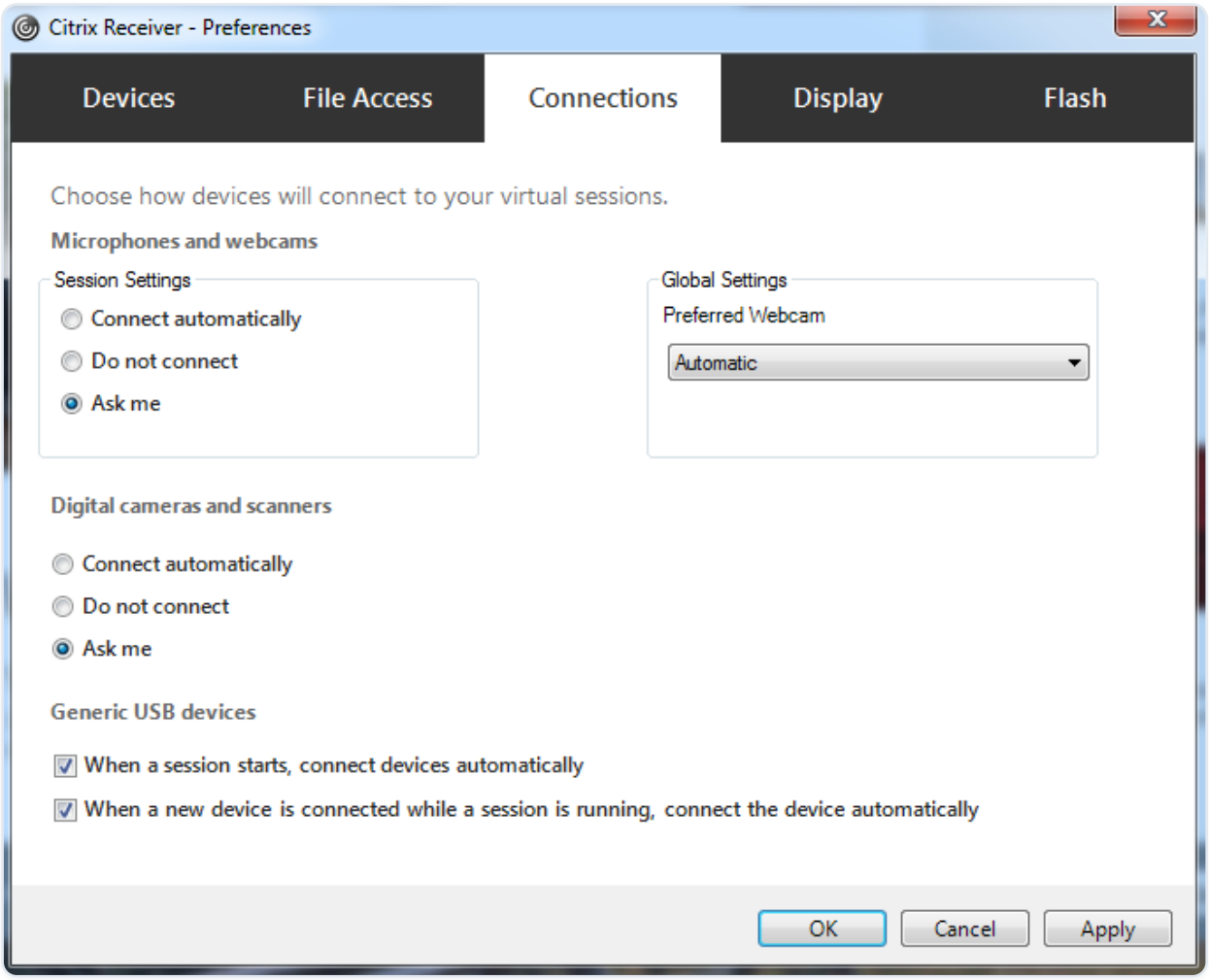


2. (Optional) To update the list of USB devices available for redirection, add the Client USB device redirection rules setting to a policy and specify the USB policy rules.

   In Citrix Workspace app:

3. Specify that devices are connected automatically without manual redirection. You can do this using an Administrative template or in Citrix Workspace app for Windows > Preferences > Connections.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If you specified USB policy rules for the VDA in the previous step, specify those same policy rules for Citrix Workspace app.

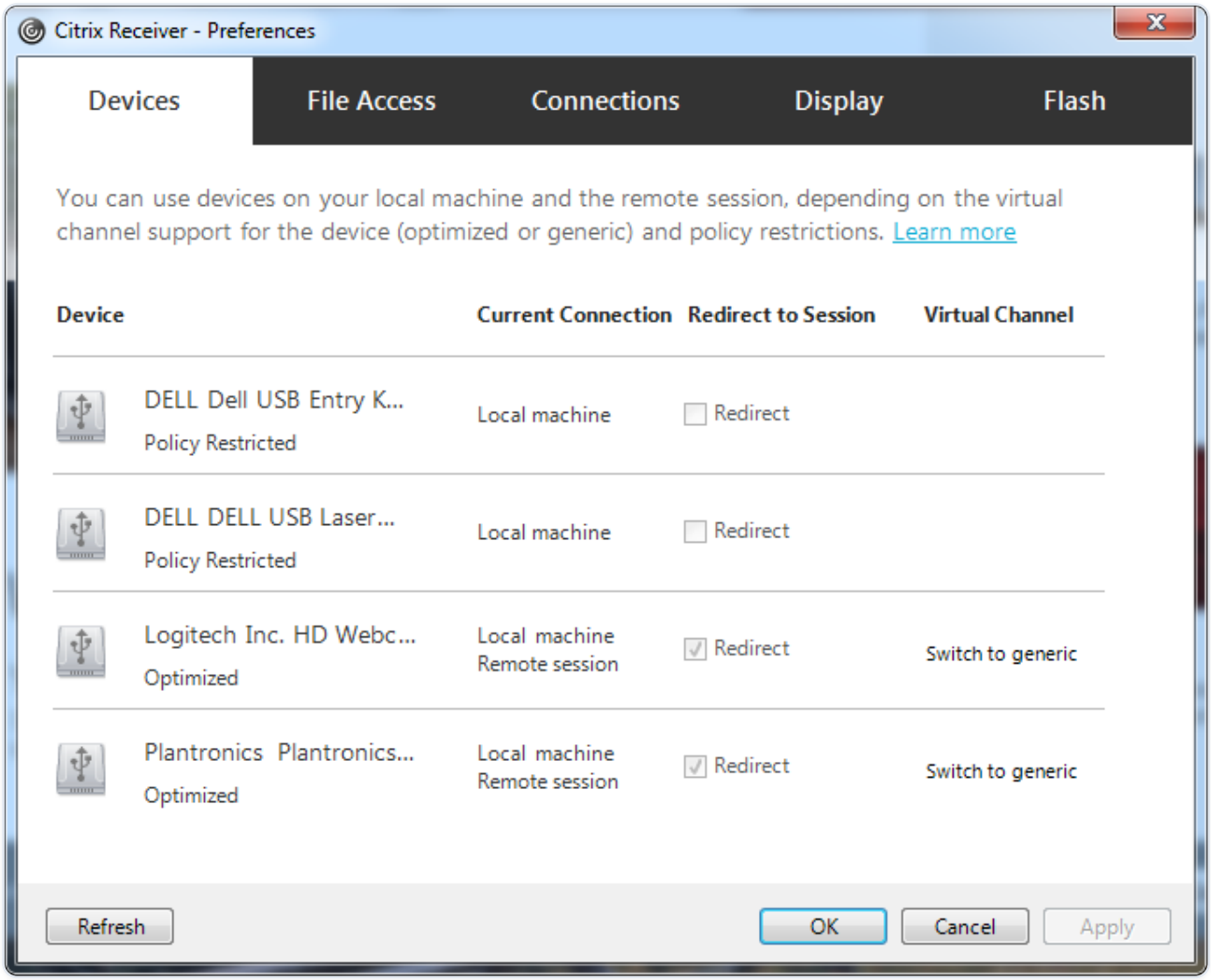
For thin clients, consult the manufacturer for details of USB support and any required configuration.

Configuring the types of USB devices available for generic USB redirection

USB devices are automatically redirected when USB support is enabled and the USB user preference settings are set to connect USB devices automatically. USB devices are also automatically redirected when the connection bar is not present.

Users can explicitly redirect devices that are not automatically redirected by selecting the devices from the USB device list. For more information, the Citrix Workspace app for Windows user help article, Display your devices in the Desktop Viewer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To use generic USB redirection rather than optimized support, you can either:

- In Citrix Workspace app, manually select the USB device to use generic USB redirection, choose **Switch to generic** from the Devices tab of the Preferences dialog box.
- Automatically select the USB device to use generic USB redirection, by configuring auto-redirection for the USB device type (for example, AutoRedirectStorage=1) and set USB user preference settings to automatically connect USB devices. For more information, see Configure automatic redirection of USB devices.

NOTE:

Only configure generic USB redirection for use with a webcam if the webcam is found to be incompatible with HDX multimedia redirection.

To prevent USB devices from ever being listed or redirected, you can specify device rules for Citrix Workspace app and the VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For generic USB redirection, you need to know at least the USB device class and subclass. Not all USB devices use their obvious USB device class and subclass. For example:

- Pens use the mouse device class.
- Smart card readers can use the vendor-defined or HID device class.

For more precise control, you need to know the Vendor ID, Product ID, and Release ID. You can get this information from the device vendor.

IMPORTANT:

Malicious USB devices might present USB device characteristics that do not match their intended usage. Device rules are not intended to prevent this behavior.

You control the USB devices available for generic USB redirection by specifying USB device redirection rules for both VDA and Citrix Workspace app, to override the default USB policy rules.

For the VDA:

- Edit the administrator override rules for the Multi-session OS machines through group policy rules. The Group Policy Management Console is included on the installation media:
  - For x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - For x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

At Citrix Workspace app for Windows:

- Edit the user device registry. An Administrative template (ADM file) is included on the installation media so you can change the user device through Active Directory Group Policy: dvd root \os\lang\Support\Configuration\icaclient_usb.adm

WARNING:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

The product default rules are stored in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. Do not edit these product default

© 1997–2026 Citrix Systems, Inc. All rights reserved.

rules. Instead, use them as a guide for creating administrator override rules, which is explained later in this article. The GPO overrides are evaluated before the product default rules.

The administrator override rules are stored in HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. GPO policy rules take the format **{Allow: | Deny:}** followed by a set of *tag=value* expressions separated by white space.

The following tags are supported:

TAG	DESCRIPTION
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor; see the USB website at `<http://www.usb.org/>` for available USB Class Codes
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating policy rules, note the following:

- Rules are case-insensitive.
- Rules can have an optional comment at the end, introduced by `#`. A delimiter is not required, and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- White space is used as a separator, but cannot appear in the middle of a number or identifier. For example, Deny: Class = 08 SubClass=05 is a valid rule, but Deny: Class=0 Sub Class=05 is not.
- Tags must use the matching operator =. For example, VID=1230.
- Each rule must start on a new line or form part of a semicolon-separated list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you are using the ADM template file, you must create rules on a single line, as a semicolon-separated list.

Examples:

- The following example shows an administrator-defined USB policy rule for vendor and product identifiers:

  ```
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
  ```

- The following example shows an administrator-defined USB policy rule for a defined class, subclass, and protocol:

  ```
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices
  ```

Use and remove USB devices

Users can connect a USB device before or after starting a virtual session.

When using Citrix Workspace app for Windows, the following apply:

- Devices connected after a session begins appear immediately in the USB menu of the Desktop Viewer.
- If a USB device is not redirecting properly, you can try to resolve the problem by waiting to connect the device until after the virtual session starts.
- To avoid data loss, use the Windows "Safely Remove Hardware" icon before removing the USB device.

Security controls for USB mass storage devices

Optimized support is provided for USB mass storage devices. This support is part of Citrix Virtual Apps and Desktops client drive mapping. Drives on the user device are automatically mapped to drive letters on the virtual desktop when users log on. The drives are displayed as shared folders that have mapped drive letters. To configure client drive mapping, use the **Client removable**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

drives setting. This setting is in the File Redirection policy settings section of the ICA policy settings.

With USB mass storage devices you can use either Client drive mapping or generic USB redirection, or both. Control them using Citrix policies. The main differences are:

FEATURE	CLIENT DRIVE MAPPING	GENERIC USB REDIRECTION
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Encrypted device access	Yes, if encryption is unlocked before the device is accessed	Yes
BitLocker To Go devices	No	No
Safe to delete device during a session	No	Yes, provided users follow operating system recommendations for safe removal

If both generic USB redirection and the client drive mapping policies are enabled and a mass storage device is inserted either before or after a session starts, it is redirected using client drive mapping. When both generic USB redirection and the client drive mapping policies are enabled and a device is configured for automatic redirection and a mass storage device is inserted either before or after a session starts, it is redirected using generic USB redirection. For more information, see Knowledge Center article CTX123015.

NOTE:

USB redirection is supported over lower bandwidth connections, for example 50 Kbps. However, copying large files doesn't work.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage

Citrix manages Citrix Virtual Apps and Desktops™ service deployments by installing and maintaining the core components and features in Citrix Cloud.

You take care of the machines (VDAs) in resource locations that deliver apps and desktops. You also manage connections to those resource locations, plus the apps, desktops, and users.

- Autoscale**:** A consistent, high-performance solution to proactively power manage your machines.
- Applications**:** Manage applications in delivery groups.
- Virtual IP and virtual loopback**:** The Microsoft virtual IP address feature provides a published application with a unique dynamically assigned IP address for each session. With Citrix virtual loopback, you can configure applications that depend on communications with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.*).
- VDA registration**:** Before a VDA can facilitate delivery of apps and desktops, it must register (establish communication) with a Cloud Connector. You can specify Cloud Connector addresses using several methods, which are described in this article. As you add Cloud Connectors, VDAs must have current information.
- Sessions**:** Maintaining session activity is critical to providing the best user experience. Several features can optimize the reliability of sessions, reduce inconvenience, downtime, and loss of productivity.
- Using Search**:** To view information about machines, sessions, machine catalogs, applications, or delivery groups in Studio, use the flexible search feature.
- IPv4/IPv6 support**:** Citrix Virtual Apps and Desktops supports pure IPv4, pure IPv6, and dual-stack deployments that use overlapping IPv4 and IPv6 networks. This article describes and illustrates these deployments. It also describes the Citrix policy settings that control the use of IPv4 or IPv6.
- Profile management**:** Citrix Profile Management can be installed when you install a VDA. If you use this user profile solution, review its documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Insight Services**:** Citrix Insight Services (CIS) is a Citrix platform for instrumentation, telemetry, and business insight generation. Analytics and diagnostics are collected when you install a VDA.
- Local Host Cache**:** Local Host Cache enables connection brokering operations to continue when a Cloud Connector in a resource location cannot communicate with Citrix Cloud. Scale, size, and other configuration considerations are also provided.
- Delegated administration**:** With delegated administration, you can configure the access permissions that all of your administrators need, according to their role in your organization.
- Configuration logging**:** Configuration logging tracks configuration changes and administrative activities.
- Event logs**:** Services within Citrix Virtual Apps and Desktops log the events that occur. Event logs can be used to monitor and troubleshoot operations.
- Licenses**:** You can view Citrix license usage information for this service from the Citrix Cloud console.
- Load balance machines**:** You can control how to load balance machines.

Adaptive access

In today's ever changing situations, application security is vital for any businesses. Making context-aware security decisions and then enabling access to the applications reduces the associated risks while enabling access to users.

The Adaptive access feature offers a comprehensive zero-trust access approach that delivers secure access to the applications. Adaptive access enables admins to provide granular level access to the apps that users can access based on the context. The term "context" refers to:

- Users and groups (users and user groups)
- Devices (desktop or mobile devices)
- Location (geo-location or network location)
- Device posture (device posture check)
- Risk (user risk score)

Device Posture service

Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (Citrix Virtual Apps™ and Desktops) or Citrix Secure Private Access resources (SaaS and Web apps or TCP and UDP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

apps). Establishing device trust by checking the device's posture is critical to implement zero-trust-based access. Device Posture service enforces zero trust principles in your network by checking the end devices for compliance (managed/BYOD and security posture) before allowing an end user to log in.

For details, see Device Posture.

Adaptive Authentication service

Adaptive Authentication is a Citrix Cloud™ service that enables advanced authentication for customers and users logging in to cloud stores. Adaptive Authentication service is a Citrix managed and Citrix Cloud hosted ADC that provides all the advanced authentication capabilities such as the following:

- Multifactor authentication using different auth methods like AD, RADIUS, certificate, multiple third-party IdPs using SAML 2.0, OAuth, OIDC, Google Captcha.
- Verify user identity and authorization levels based on factors such as location, device status, and user group.
- Enable contextual or smart access to DaaS (virtualized) and SPA (non-virtualized resources like Web and SaaS apps).
- Login page customization

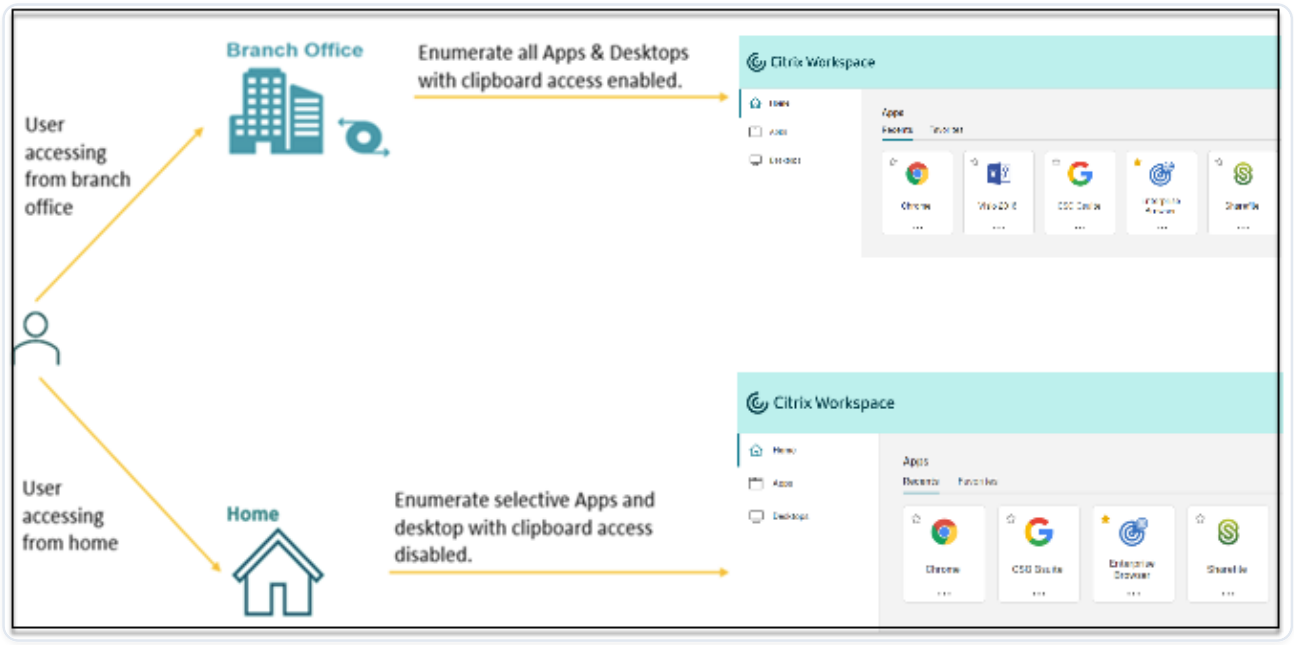
For complete details about Adaptive Authentication, see Adaptive Authentication service.

Adaptive access based on user's network location

The Citrix® StoreFront Cloud Adaptive Access feature uses advanced policy infrastructure to enable access to Citrix DaaS™ based on the user's network location. The location is defined using the IP address range or subnet addresses.

Admins can define policies to either enumerate or not enumerate virtual apps and desktops based on the user's network location. Admins can also control the user actions by enabling or disabling clipboard access, printers, client drive mapping and so on, based on the user's network location. For example, admins can set up policies such that users accessing the resources from home have limited access to applications and users accessing the resources from branch offices have full access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



An admin can implement the following policies for accessing the applications:

- Enumerate a few sensitive applications only from corporate location or from their branch offices.
- Do not enumerate sensitive applications if the employees are accessing the workspace from an outside network.
- Disable printer access from the branch offices.
- Disable clipboard access and printer access when the users are outside the corporate network.

Entitlements

The Adaptive Access feature is available as part of Universal Hybrid Multi Cloud License (UHMC) and Platform License (CPL). For more information, see `<https://www.citrix.com/buy/licensing/product.html>`.

Prerequisites

- Ensure that the **Adaptive Access** feature is enabled (**StoreFront Cloud > Access > Adaptive Access**). For details, see Enable the Adaptive Access feature.

  When adaptive access is enabled, the DaaS access policies are updated to use the option **Connections through Citrix Gateway**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

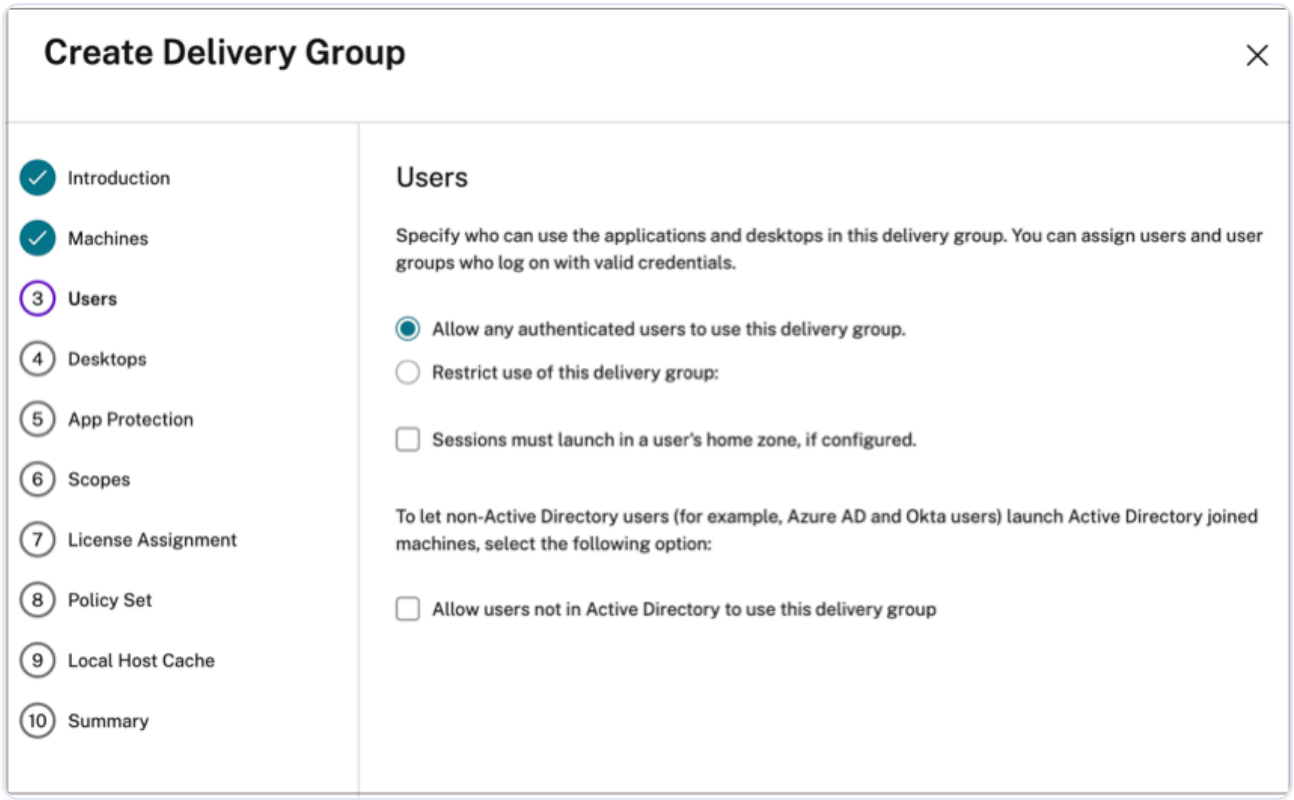
NetScaler® Gateway is required to add smart access tags in DaaS access policies. However, because DaaS consumes tags from Device Posture, Adaptive Access, and Adaptive Authentication services, it isn't necessary to have a configured NetScaler Gateway in your setup.

- Understanding of location tags. For details, see Network Location tags.

Points to note

The following points are only applicable if you want to restrict application enumeration based on the location. If you plan to use adaptive access to restrict user controls like disabling clipboard access, printer redirection, client drive mapping, based on the network location, you can ignore these guidelines.

- If you plan to selectively enumerate Citrix DaaS based on network location, then user management must be performed for those delivery groups using Citrix Studio policies instead of workspace. When creating a Delivery group, in **Users setting**, either choose **Restrict use of this Delivery Group** users or **Allow any authenticated users to use this Delivery Group**. This enables you to configure adaptive access in the **Access Policy** tab under **Delivery Group**.

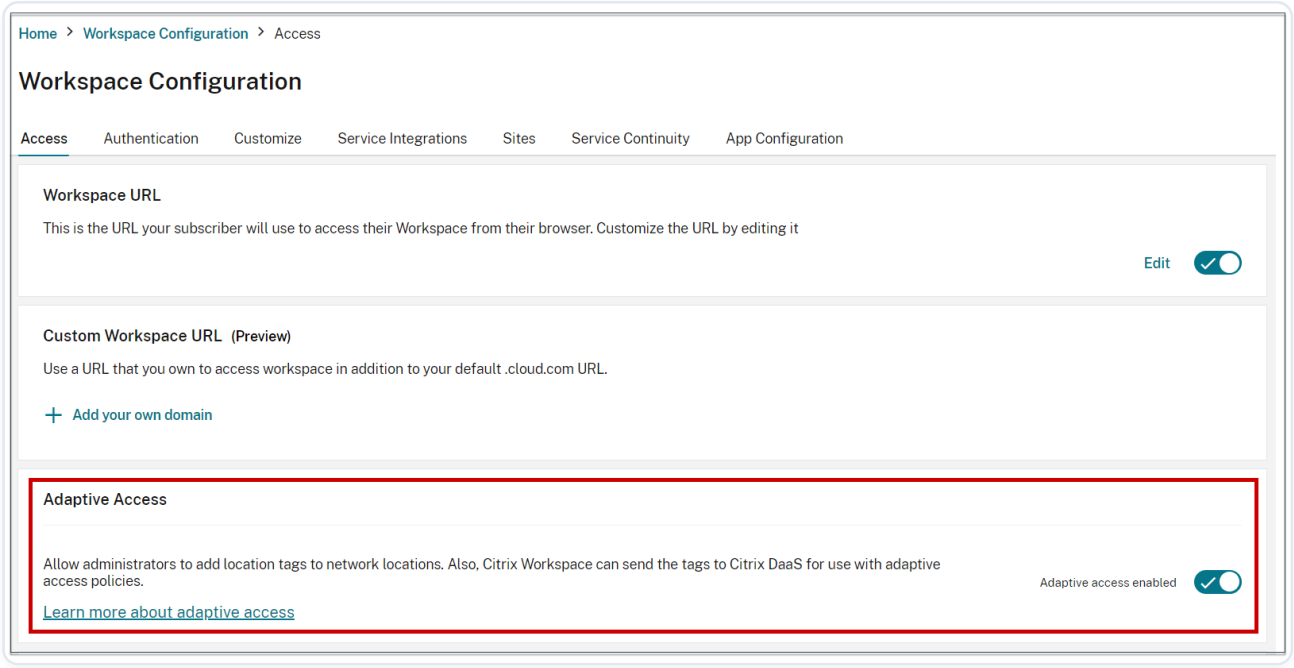


© 1997–2026 Citrix Systems, Inc. All rights reserved.

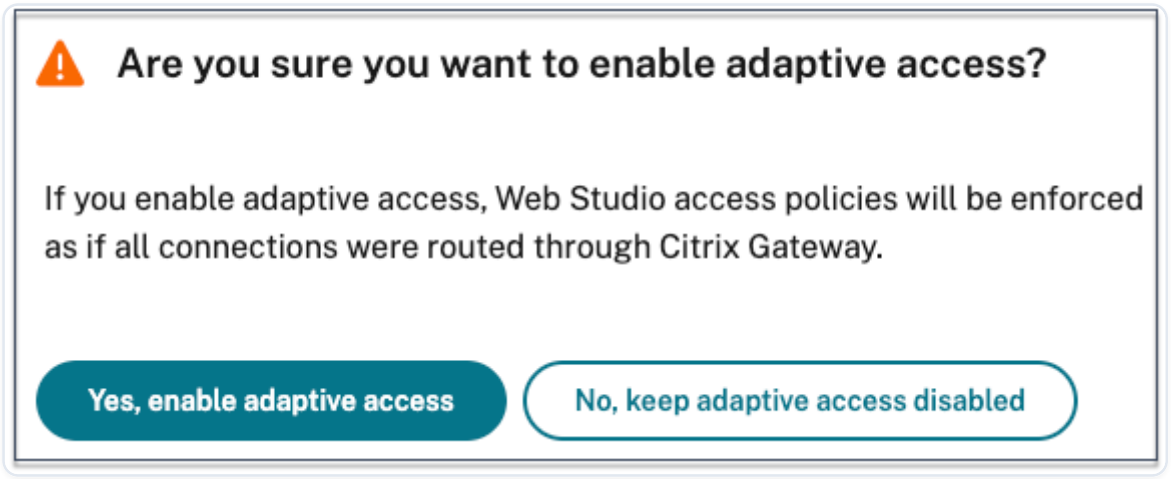
- Changes to Direct Workload Connection when adaptive access is enabled.
  - The **Location tags** field is visible in **Citrix Cloud™ > Network Locations > Add a Network Location > Location tags**.
  - Existing Direct Workload Connection policies work as intended.
  - New policies must be created in the Network Locations service (without defining tags) and also on the delivery group. In addition, the network connectivity type must be **Internal**.
  - For new policies for Direct Workload Connection with tags, tags must be defined in the Network Locations service and also the same tags must be defined on the delivery group or access policy in DaaS Studio. In addition, the network connectivity type must be **Internal**. Location tags aren't relevant for Direct Workload Connection.
- The following is recommended testing your Citrix DaaS deployment.
  - Identify a test delivery group or create a delivery group to implement this capability.
  - Create a policy or identify a policy that can be used with a test delivery group.

Enable the Adaptive Access feature

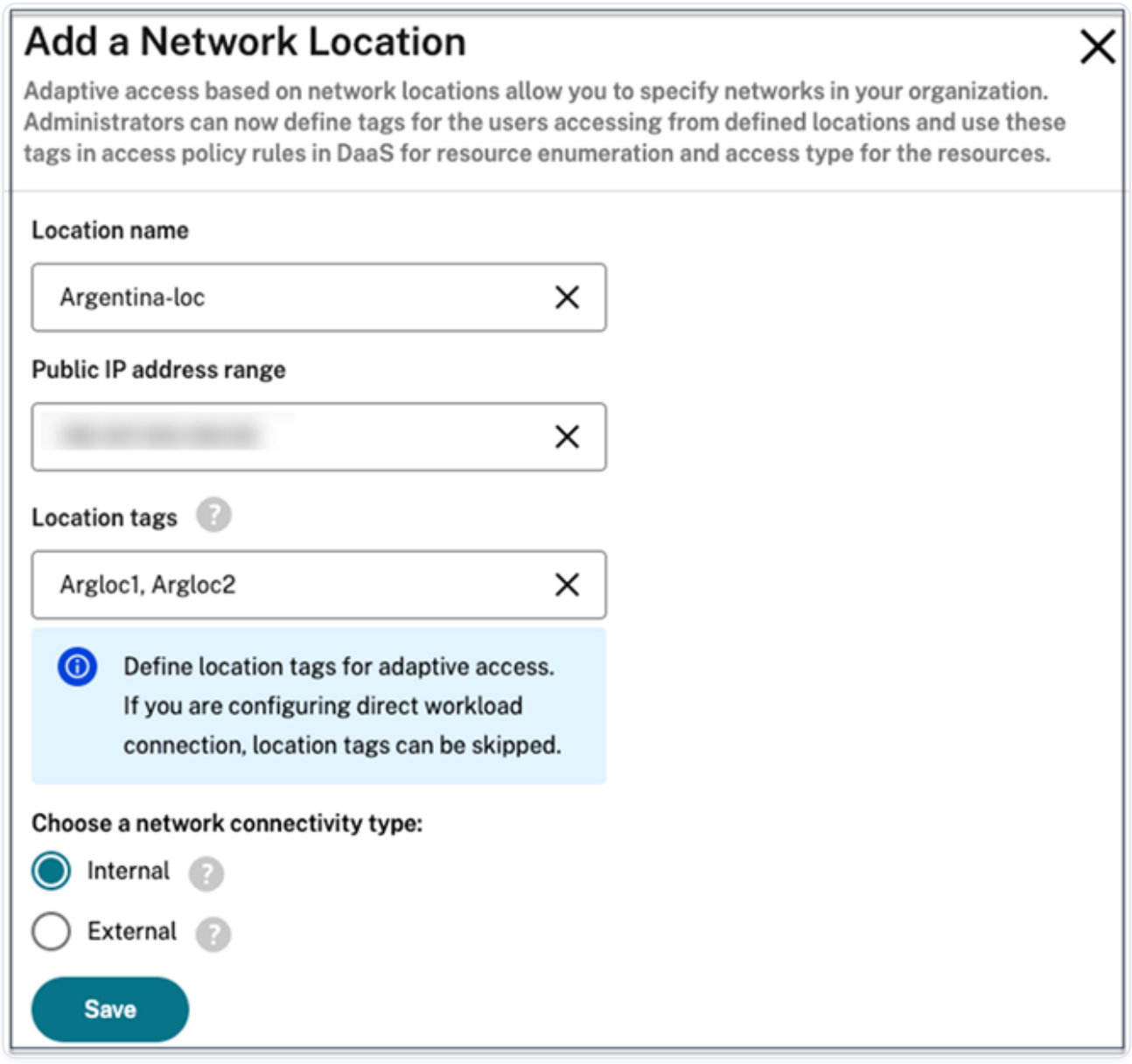
1. Log in to Citrix Cloud.
2. Select **StoreFront Cloud** from the hamburger menu.
3. **Adaptive Access** toggle is turned off, by default. Turn the **Adaptive Access** toggle on.
4. Click **Yes, enable adaptive access** on the confirmation message.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

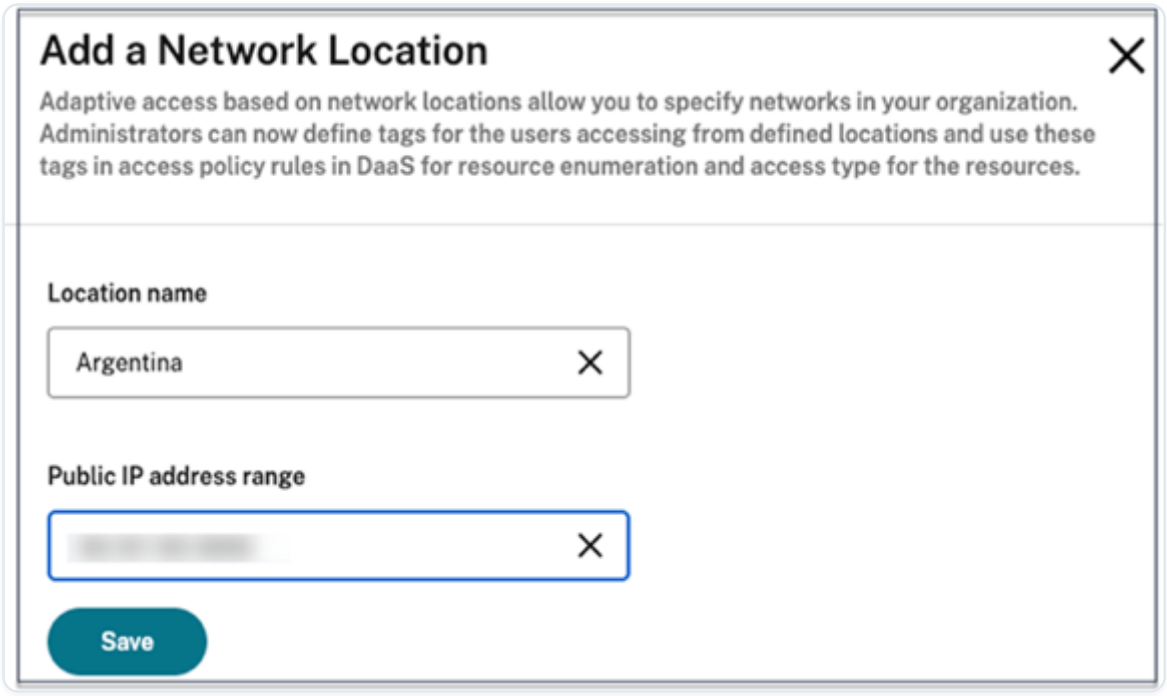


When adaptive access is enabled, you can define the location tags for adaptive access (**Citrix Cloud > Network Locations > Add a Network Location > Location tags**).



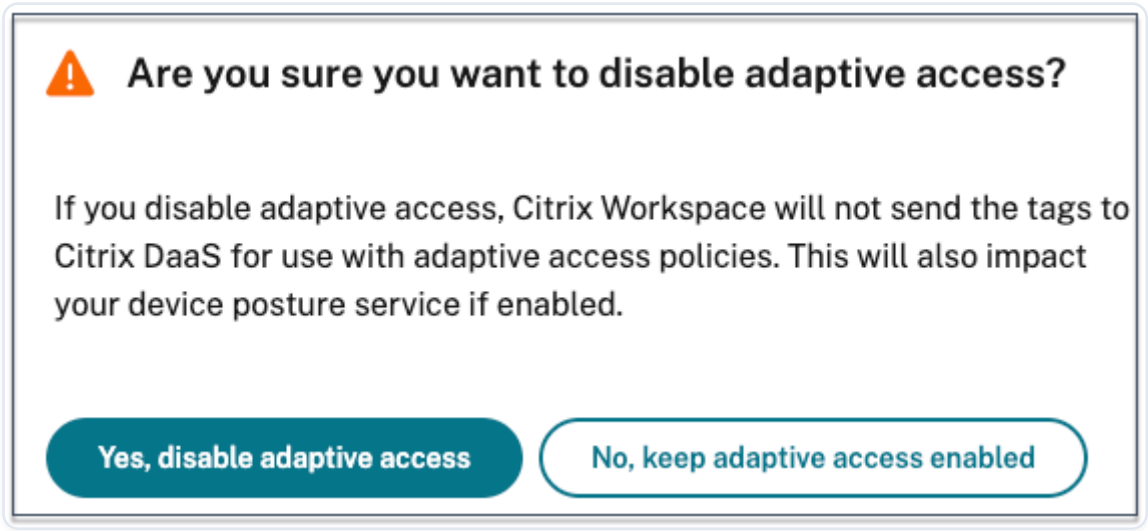
When Adaptive Access is disabled, you can't add a network location. Location tags aren't applicable in this case.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



IMPORTANT:

When you try to disable the Adaptive Access feature, the following message appears. Note that Workspace does not send the tags to the DaaS for adaptive access when the feature is disabled.



Configure adaptive access

Consider a scenario where an administrator needs to enforce access control based on the users' network locations (for example office and home). Admin must also enforce smart controls such as clipboard restrictions for users working from home. To achieve this scenario with Adaptive access, admin must create 2 delivery groups based on the user's network:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Adaptive Access** delivery group for BranchOffice with applications relevant to branch office users.
- **WFH** delivery group for WorkFromHome with applications relevant to home/remote users.

After the delivery groups are created, the following high-level steps are involved in configuring adaptive access based on network locations:

- Define tags and configure the network location policies.
- Use the defined tags in delivery groups for application enumeration and or Enforce smart controls on applications.
- Enforce smart controls on applications (optional).

Define network location tags for location-based access

The first step involves defining tags for users based on their locations; office or home.

- **BRANCHOFFICE:** This tag must be assigned to users connecting from the office network. These users have full access to all applications available to them.
- **WORKFROMHOME:** This tag must be assigned to users working remotely. These users have limited access to applications and certain features (like clipboard functionality).

For more information about tags, see Network Location tags.

Now that you have the delivery groups and respective tags created based on user location, you can proceed to network location policy configuration.

Configure the network location policies

Define network location policy rules for your user's location by providing the public source IP address and location tag.

1. Sign into Citrix Cloud.
2. Select **Network Locations** from the hamburger menu. Ensure that the Adaptive Access toggle is enabled. Else the user interface for the Direct Workload Connection is displayed.
3. Click **Add network location**.
    - **Location name:** Enter an appropriate name for the policy.

      Example: BRANCHOFFICE or WORKFROMHOME
    - **Public IP address range:** Define the public IP address range for your network.

      Example: 192.0.2.10 - 192.0.2.30

© 1997–2026 Citrix Systems, Inc. All rights reserved.

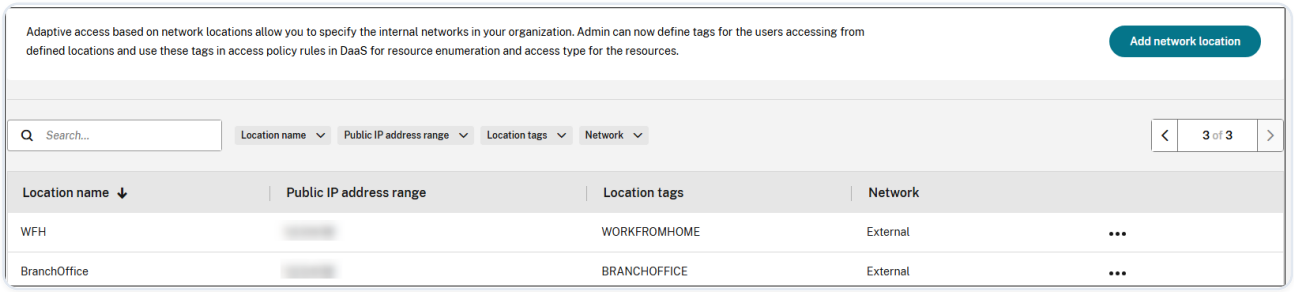
- **Location Tags:** Define tags for your location. This can be a name referring to your location. These tags are used to configure the adaptive access policies in Citrix Studio. For details, see **Define tags in Citrix Studio**.

  Example: BRANCHOFFICE or WORKFROMHOME

- **Connectivity type:** Define the application launch type.

  Internal - Bypass gateway for application launch. **External** - Use Citrix Gateway service or traditional gateway for application launch.

4. Click **Save**.



You can now use these tags on DaaS Studio to enable adaptive access.

NOTE:

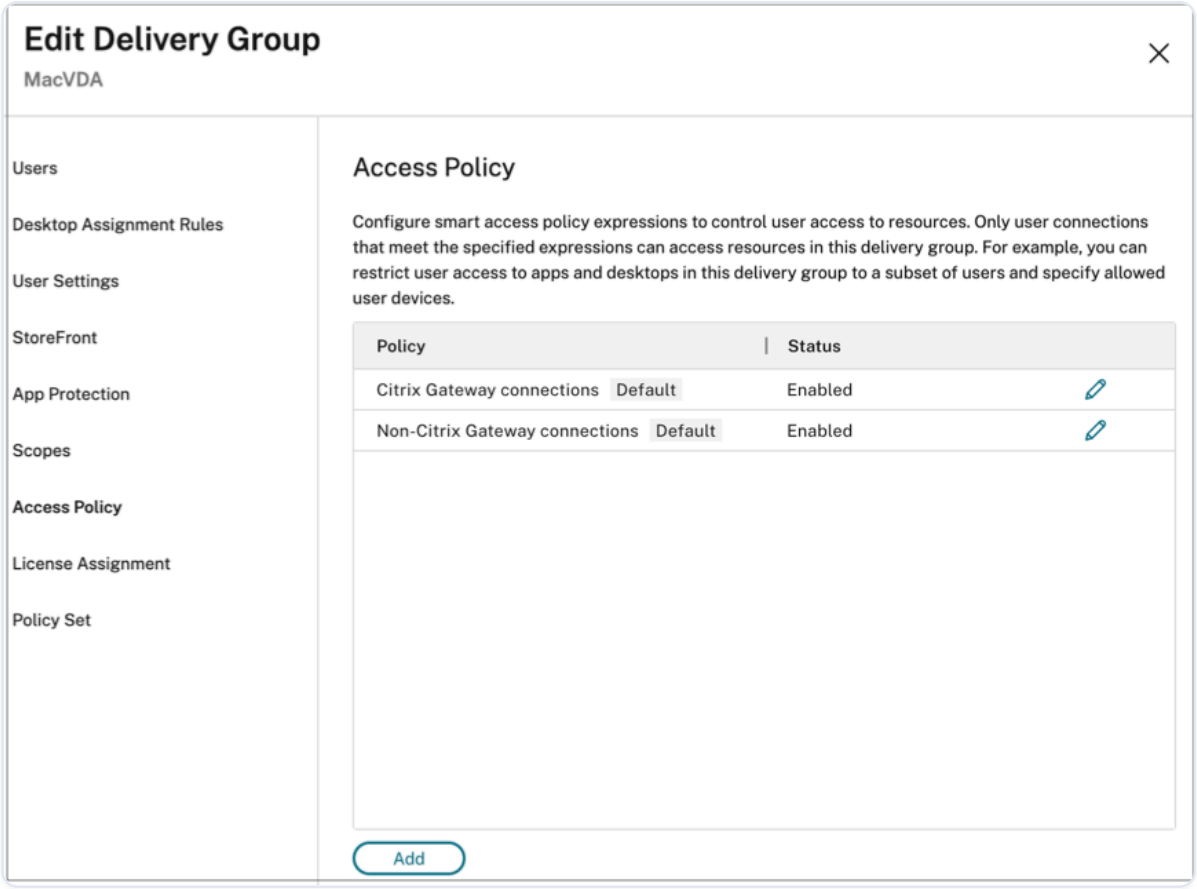
- If network location tags are not assigned to the delivery groups, the users are granted unrestricted access to all applications in both Adaptive Access and WFH delivery groups. This might result in scenarios where users might inadvertently access certain applications that they are not authorized to. Assigning location tags to delivery groups ensures that access is controlled based on the users' network location.
- While defining the location tags, ensure that you only enter the preferred tag name without the prefix "LOCATION_TAG", for example BRANCHOFFICE. However, while defining tags in Citrix Studio, you must prefix the tag name with "LOCATION_TAG". For example, "LOCATION_TAG_BRANCHOFFICE".

Use the defined tags in delivery groups for application enumeration

1. Sign into Citrix Cloud.
2. On the **Citrix DaaS** tile, click **Manage**.
3. Create a delivery group. For details, see Create delivery groups.
4. Select the delivery group that you've created, and click **Edit Delivery Group**.

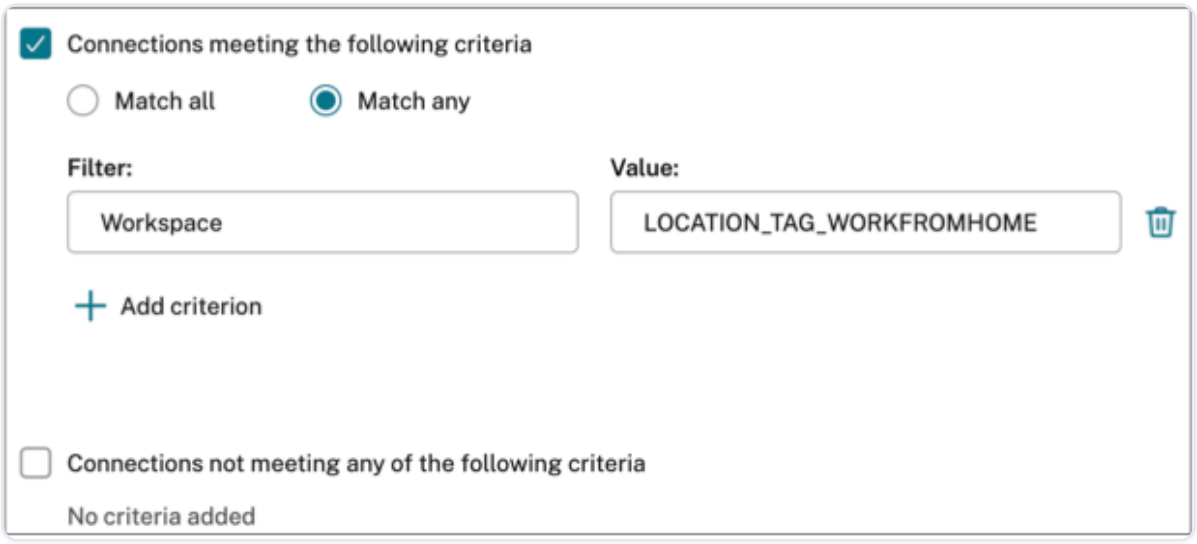
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **Access Policy**.
6. For customers using adaptive access, perform the following steps to restrict access for a delivery group to internal networks only:
   a. Right-click the delivery group and select **Edit**.
   b. Select the access policy in the left pane.
   c. Click the edit icon to modify the default Citrix Gateway connections policy.



   d. On the **Edit policy** page, select **Connections meeting the following criteria**, select **Match any**, and then add the criteria.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For WorkFromHome users, enter the following values in the respective delivery controller.

Filter: Workspace

Value: LOCATION_TAG_WORKFROMHOME

For BranchOffice users, enter the following values in the respective delivery controller.

Filter: Workspace

Value: LOCATION_TAG_BRANCHOFFICE

NOTE:

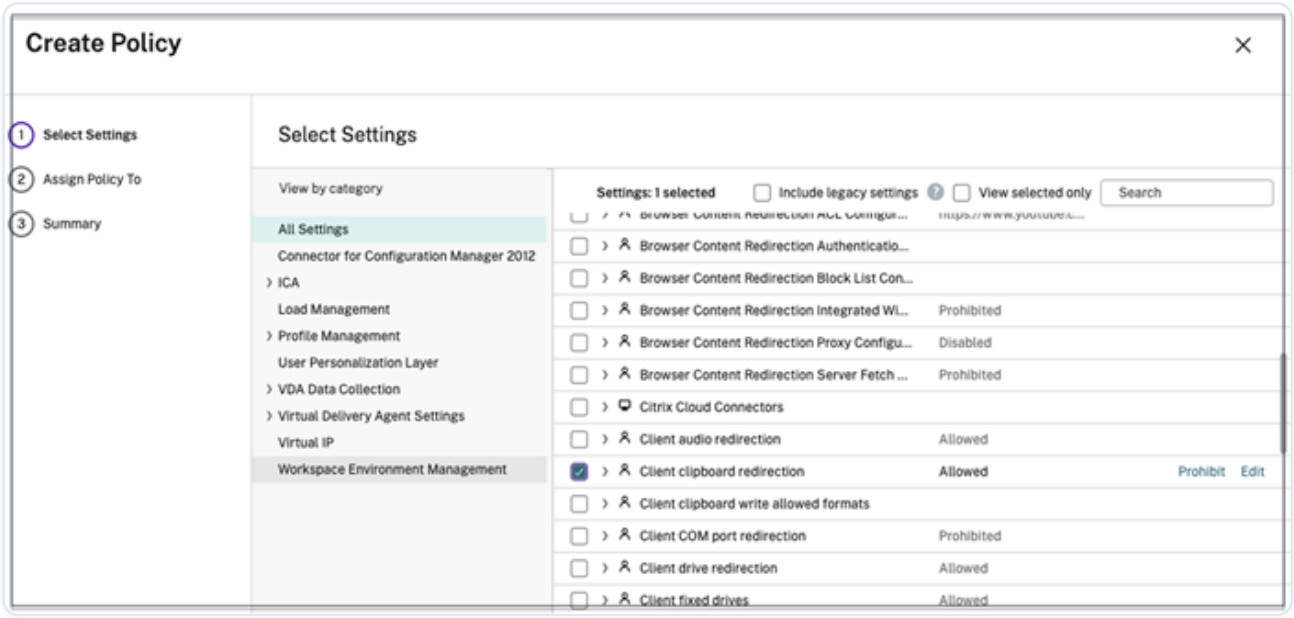
- Ensure that in the **Value** field, you enter the correct location tag name as you have defined while creating network location policies prefixed by "LOCATION_TAG". For example, if you have defined the location tag as "BRANCHOFFICE", then you must enter "LOCATION_TAG_BRANCHOFFICE" in the **Value** field. The network location tags in delivery groups must be entered in upper case irrespective of how it was defined in the network location policy. For details on configuring location tags, see Configure network location policies.
- The network location tags in delivery groups must be entered in upper case irrespective of how it was defined in the network location policy. For details on configuring location tags, see Configure the network location policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(Optional) Enforce smart controls on applications

In addition to restricting access using network location tags, admins can also enforce smart controls on applications. In this example, client clipboard redirection is disabled for users from the WorkFromHome location.

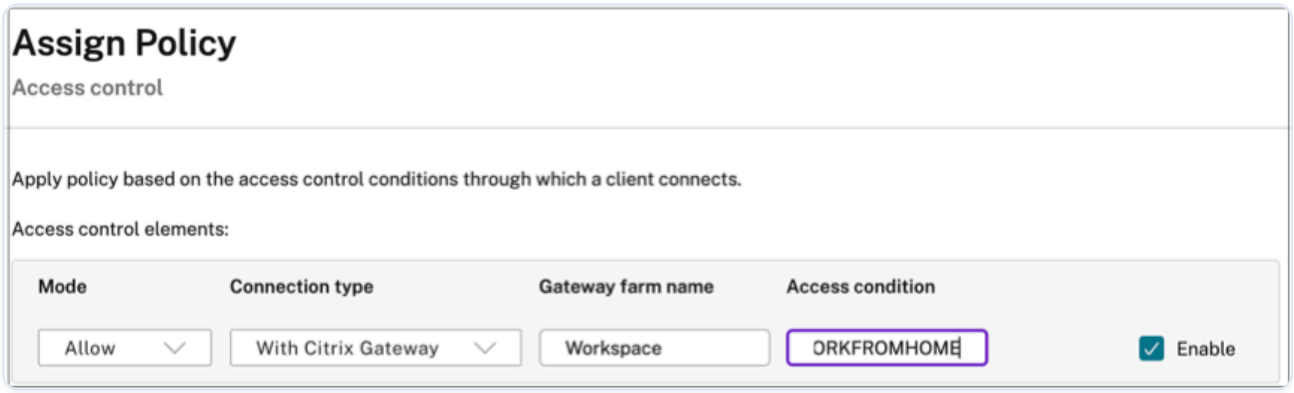
1. Sign into Citrix DaaS.
2. Navigate to **Policies** and click **Create Policy**.
3. Select **Client clipboard redirection**, and then click **Prohibit**.
4. Click **Next**.



1. On the **Assign policy To** page, select **Access control**.
2. Define the following values for the policy:

    - Mode: **Allow**
    - Connection type : **With Citrix Gateway**
    - Gateway farm name: **Workspace**
    - Access Condition: **LOCATION_TAG_WORKFROMHOME** (all in upper case)

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Click **Next**.
2. Enter a name for the policy and add a policy description.
3. Click **Finish**.

Users from the **WORKFROMHOME** location can't perform clipboard access to their launched resources.

Network location tags

The Network Locations service provides the following tags.

- **Default tags:** These tags are defined on the Network Locations service. The following default tags are available.
  - **LOCATION_internal:** Tag sent by default when the network connectivity type is set as **Internal** while defining a network location.
  - **LOCATION_external:** Tag sent by default when the network connectivity type is set as **External** while defining a network location.
  - **LOCATION_undefined:** Tag sent for an IP address that is not defined in the policy but is coming through the Network Locations service. Launch for these users are the same as what is defined in the resource group.
- **Custom tags:** Admins can define custom tag names in the policies. Example: home, Office, BRANCH

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- When defining tags for the Network Location service, ensure the following:

  The default tags always start with the prefix "LOCATION_`<tag name>`. For example, LOCATION_INTERNAL.

  The custom tags always start with the prefix "LOCATION_TAG`<tag name>`. For example, LOCATION_TAG_OFFICE.

- When defining tags in the delivery groups, tags must be entered in all upper case.

  Default tags: LOCATION_INTERNAL, LOCATION_EXTERNAL, LOCATION_UNDEFINED

  Custom tags: LOCATION_TAG_OFFICE, LOCATION_TAG_HOME

The following table summarizes the policies and tags for the earlier mentioned scenario.

LOCATION	POLICY	CUSTOM TAG	DEFAULT TAG	TAG TO BE USED IN DAAS DELIVERY GROUP	TAGS TO BE USED IN THE SMART ACCESS POLICY
WFH	WFH	WORKFROMHOME	LOCATION_EXTERNAL	LOCATION_WORKFROMHOME and/or LOCATION_EXTERNAL	LOCATION_WORKFROMHOME and/or LOCATION_EXTERNAL
BranchOffice	BranchOffice	BRANCHOFFICE	LOCATION_EXTERNAL	LOCATION_BRANCHOFFICE and/or LOCATION_EXTERNAL	LOCATION_BRANCHOFFICE and/or LOCATION_EXTERNAL
Other	Not defined	Not defined	LOCATION_UNDEFINED	LOCATION_UNDEFINED	LOCATION_UNDEFINED

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issues

If you disable the Adaptive Access feature after it was enabled and the rules were set (tags and connectivity type), this does not remove the locations from the Network Locations page though the location tags and the connectivity type columns are hidden. But these locations are disabled in the back-end. This is a cosmetic issue.

Configure session recording policies based on tags

Session Recording allows organizations to record on-screen user activity in virtual sessions. You can specify tags including network location tags when creating a custom session recording policy, event detection policy, or event response policy. For an example, see Create a custom recording policy.

Applications

Introduction

If your deployment uses only delivery groups (and not application groups), add applications directly to the delivery groups. When application groups are available, it’s better to add applications to them instead, because this practice simplifies administration. Every application must be associated with at least one delivery group or application group.

In the **Add Applications** wizard, you can select one or more delivery groups, or one or more application groups, but not both. Although you can later change an application's group association (for example, moving an application from an application group to a delivery group), best practice discourages adding that complexity. Keep your applications in one type of group.

When you associate an application with more than one group, a visibility issue can occur if you do not have sufficient permission to view the application in all of those groups. In such cases, either consult an administrator with greater permissions or have your scope extended to include all the groups with which the application is associated.

If you publish two applications with the same name (perhaps from different groups) to the same users, change the `Application name (for user)` property in Studio. Otherwise, users see duplicate names in Citrix Workspace™ app.

You can change an application's properties (settings) when you add it, or later. You can also change the application folder where the application is placed, either when you add the application, or later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add applications

You can add applications when you create or edit a delivery group or application group. The following procedure describes how to add applications after you create a group.

Good to know:

- You cannot add applications to Remote PC Access delivery groups.
- You cannot use the **Add Application** wizard to remove applications from delivery groups or application groups. That is a separate operation.

Add one or more applications to multiple delivery groups or application groups

To add applications to multiple groups, follow these steps:

1. In the left pane, choose where you want to add the applications:
    - To add to a delivery group, click **Delivery groups** and then select the target delivery group.
    - To add to an application group, click **Applications**, select the **Application group** tab, and then select the application group.
2. Select **Add Applications** in the action bar. The Add Applications wizard launches with an **Introduction** page. Click **Next**.
3. Follow the steps in the wizard to configure the settings:
    a. On the **Group** page, choose the delivery groups and applications group where you want to add applications, then click **Next**. For more information, see Select groups.
    b. On the **Applications** page, Specify the applications you want to add, and then click **Next**. For more information, see Specify applications.
    c. On the **Summary** page, Review the settings:
        - If you are adding 10 or fewer applications, their names are listed in **Applications to add**
        - If you are adding more than 10 applications, the total number is specified.
    d. Click **Finish**.

Add one or more applications to a delivery group or application group

To add applications to a group, follow these steps:

1. In the left pane, choose where you want to add the applications:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To add to a delivery group, click **Delivery groups** and then select the target delivery group.
- To add to an application group, click **Applications**, select the **Application group** tab, and then select the application group.

2. Select **Add Applications** in the action bar.
3. Follow the steps in the wizard to configure the settings:

   a. On the **Applications** page, Specify the applications you want to add, and then click **Next**. For more information, see Specify applications.

   b. On the **Summary** page, Review the settings:

      - If you are adding 10 or fewer applications, their names are listed in **Applications to add**
      - If you are adding more than 10 applications, the total number is specified.

   c. Click **Finish**.

Select groups

The **Groups** page in the **Add Applications** wizard lists all delivery groups in the site. If application groups exist, both application groups and delivery groups are listed.

You can select either delivery groups or application groups—but *not both* at the same time. That is, you cannot add applications to a delivery group and an application group in the same operation. If you're using application groups, we recommend adding applications to those application groups instead of to delivery groups.

Select the checkbox next to at least one group. Each application must be associated with at least one group.

Specify applications

The **Applications** page in the **Add applications** wizard lets you specify which applications to add to the selected group or groups.

Click **Add** to display the application sources.

- **From Start menu:** Applications that are discovered on a machine in the selected delivery groups. When you select this source, a new page launches with a list of discovered applications. Select the checkboxes of applications to add, and then click **OK**.

  This source cannot be selected if you:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Select application groups with no associated delivery groups.
    - Select application groups with associated delivery groups that contain no machines.
    - Select a delivery group containing no machines.

- **Manually:** Applications on a VDA in the delivery group or elsewhere in your network. Selecting this source opens a new page where you specify an application to add in the following ways:

    - Type the path to the executable, working directory, optional command line arguments, and display names for administrators and users.
    - Select an application from a VDA in the delivery group. To do so, click **Browse**, enter credentials for accessing the VDA, wait to be connected to the VDA, and then select an application from the VDA. The properties of the selected application automatically populate fields on the page.

- **Existing:** Applications previously added to the site. When you select this source, a new page launches with a list of discovered applications. Select the checkboxes of applications to add and then click **OK**.

  This source cannot be selected If the site has no applications.

- **App packages:** Applications in the App-V, MSIX, MSIX app attach, or FlexApp application packages. When you select this source, the **Add Applications from Packages** page launches. Select an application package source, select the applications you want to add from the resulting display, and then select **OK**. For more information, see Deploy and deliver App-V applications.

- **Application Group**: Application groups. When you select this source, a new page launches with a list of application groups. (Although the display also lists the applications in each group, you can select only the group, not individual applications.) All current and future applications in the selected groups are added. Select the checkboxes of application groups to add, and then click **OK**.

  This source cannot be selected if (1) there are no application groups, or (2) if the selected delivery groups do not support application groups (for example, delivery groups with statically assigned machines).

As noted in the table, some sources in the **Add** list cannot be selected if there is no valid source of that type. Sources that are incompatible (for example, you cannot add application groups to application groups) are not included in the list. Applications that are already added to the groups you chose cannot be selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can change an application's properties (settings) from this page, or later.

By default, added applications are placed in the application folder named `Applications`. You can change the application from this page, or later.

If you try to add an application and one with the same name exists in the same folder, you are prompted to rename the application you're adding. You can accept the new name offered, or decline and then rename the application or select a different folder.

For example, if `app` exists in the **Applications** folder, and you attempt to add another application named `app` to that folder, the new name `app_1` is offered.

Change an application's group association

After adding an application, you can change the delivery groups and application groups with which the application is associated.

You can drag an application to an additional group. This is an alternative to using commands in the action bar.

If an application is associated with more than one delivery group, either using an application group or directly, group priority can be used to specify the order in which multiple groups are evaluated.

Groups can be excluded from consideration based on factors like access policy, user lists, or smart access tags, and the specific machine chosen from the group can be affected by factors like zone preference, and launch readiness, and any tag restrictions. By default, all groups are priority 0 (the highest). If the delivery groups have equal priority, then the least loaded delivery group is selected for launching the application. The vertical load balancing is not considered in this case.

An application can be associated with delivery groups containing shared (not private) machines that can deliver applications. You can also select delivery groups containing shared machines that deliver desktops only, if:

- The delivery group contains shared machines and was created with a XenDesktop 7.x version earlier than 7.9
- You have `Edit delivery group` permission. The delivery group type is automatically converted to `desktops and applications` when the properties dialog is committed.

1. Select **Applications** in the left pane, and then select the application.
2. Select **Properties** in the action bar.
3. Select the **Groups** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To add a group, click **Add** and select **Application Groups** or **Delivery Groups**. (If you have not created any application groups, the only entry is **Delivery Groups**.) Then, select one or more available groups. Groups that are incompatible with the application, or that are already associated with the application, cannot be selected.
- To remove a group, select one or more groups and then click **Remove**. If removing a group association results in the application no longer being associated with any group, you are alerted that the application will be deleted.
- To change the priority of a group, select the group and then click **Edit Priority**. Select a priority value and then click **OK**.

4. When you are finished, click **Apply** to apply the changes and leave the window open, or click **OK** to apply the changes and close the window.

Change application properties

You can change the properties of only one application at a time.

To change the properties of an application:

1. Select **Applications** in the left pane.
2. Select an application and then select **Properties** in the action bar.
3. In the left pane, select the page containing the property that you want to change.
4. When you are finished, click **Apply** to apply any changes you made and keep the window open, or click **Save** to apply changes and close the window.

PAGE NAME	DESCRIPTION	
Identification	Specify app description and names: • Application names seen by the user and by the administrator. • Description and if needed, keywords for StoreFront.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PAGE NAME	DESCRIPTION
Delivery	Specify how this application is delivered to users: • Icon • Category or folder where an application appears in their store. • Whether to create a shortcut on the user's desktop. • Limits. see Configure application limits. • Visibility of packaged applications: Citrix Virtual Desktops, Citrix Virtual Apps, or both.
Location	Specify the following location: • Path to executable; see Pass parameters to published applications. • Command line arguments; see Pass parameters to published applications. • Working directory
Groups	Add, remove, or change the priority of the delivery or application groups where the application is available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PAGE NAME	DESCRIPTION
Limit Visibility	Control which users can see the application in the Citrix Workspace app. An invisible application can still be started. To make it unavailable and invisible, add it to a different group. **Note:** Currently, this feature is available only for AD and Microsoft Entra users. For Microsoft Entra users, app visibility limitation requires VDA version 2411 or later.
File Type Association	Specify which extensions the application opens automatically.
Zone	When your site includes multiple zones, specify whether zones affect the application launch.

Application changes might not take effect for current application users until they log off from their sessions.

Configure application limits

Configure application limits to help manage application use. For example, you can use application limits to manage the number of users accessing an application simultaneously. Similarly, application limits can be used to manage the number of simultaneous instances of resource-intensive applications. That limit can help maintain server performance and prevent deterioration in service.

This feature limits the number of application launches that are brokered by the Controller (for example, from Citrix Workspace app and StoreFront), and not the number of running applications that can be launched by other methods. This means that application limits assist administrators

© 1997–2026 Citrix Systems, Inc. All rights reserved.

when managing concurrent usage, but do not provide enforcement in all scenarios. For example, application limits cannot be applied when the Controller is in outage mode.

By default, there is no limit on how many application instances can run at the same time. There are several application limit settings. You can configure any or all of them.

- The maximum number of concurrent instances of the application by all users in the delivery group.
- One instance of the application per user in the delivery group.
- The maximum number of concurrent instances of the application per machine (PowerShell only).

If a limit is configured, an error message is generated when a user attempts to launch an instance of the application that will exceed the configured limit. If more than one limit is configured, an error is reported when the first limit is reached.

Examples using application limits:

- **Maximum number of simultaneous instances limit:** In a delivery group, you configure the maximum number of simultaneous instances of application `Alpha` to 15. Later, users in that delivery group have 15 instances of that application running at the same time. If any user in that delivery group now attempts to launch `Alpha`, an error message is generated. `Alpha` is not launched because it would exceed the configured simultaneous application instance limit (15).
- **One-instance-per-user application limit:** In another delivery group, you enable the one-instance-per-user option for application `Beta`. User Tony launches application `Beta` successfully. Later in the day, while that application is still running in Tony's session, he attempts to launch another instance of `Beta`. An error message is generated and `Beta` is not launched because it would exceed the one-instance-per-user limit.
- **Maximum number of simultaneous instances and one-instance-per-user limits:** In another delivery group, you configure a maximum number of simultaneous instances of 10 and enable the one-instance-per-user option for application `Delta`. Later, when 10 users in that delivery group each have an instance of `Delta` running, any other user in that delivery group who tries to launch `Delta` will receive an error message. `Delta` is not launched. If any of the 10 current `Delta` users attempt to launch a second instance of that application, they will receive an error message and the second instance will not be launched.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Maximum number of simultaneous instances per machine, and using tag restrictions:** Application `Charlie` has licensing and performance requirements that dictate how many instances can be running at the same time on a specific server. Those requirements also dictate how many instances can be running simultaneously across all servers in the site.

  The application instances-per-machine limit affects any server in the site (not just machines in a particular delivery group). Let's say your site has three servers. For application `Charlie`, you configure the app instances per machine limit to 2. So, no more than six instances of application `Charlie` are allowed to launch site-wide. (That's a limit of two instances of Charlie on each of the three servers.)

  To restrict an application's usage to only certain machines within a delivery group (in addition to limiting the instances on all machines site-wide):

  - Use the tagging functionality for those machines.
  - Configure the maximum number of instances per machine limit for that application.

If applications are launched by methods other than Controller brokering (for example, while a Controller is in outage mode) and configured limits are exceeded, users cannot launch more instances until they close enough instances to no longer exceed the limits. The instances that exceeded the limit are not forcibly shut down. They are allowed to continue until their users close them.

If you disable session roaming, then disable the one-instance-per-user application limit. If you enable the one-instance-per-user application limit, do not configure either of the two values that allow new sessions on new devices. For information about roaming, see Sessions.

To configure the maximum instances per delivery group limit, and the one-instance-per-user limit:

1. Select **Applications** in the left pane and then select an application.
2. Select the **Properties** in the action bar.
3. On the **Delivery** page, choose one of the following options.

   - **Allow unlimited use**. There is no limit to the number of instances running at the same time. This is the default.
   - **Set limits for the application**. There are two limit types; specify either or both.

     - Specify the maximum number of instances that can run concurrently per machine
     - Limit to one instance of the application per user

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **OK** to apply the change and close the dialog box, or **Apply** to apply the change and leave the dialog box open.

To configure the maximum instances per machine limit (PowerShell only):

- In PowerShell (using the Remote PowerShell SDK for Citrix Cloud™ deployments, or the PowerShell SDK for on-premises deployments), enter the appropriate `BrokerApplication` cmdlet with the `MaxPerMachineInstances` parameter.
- For guidance, use the `Get-Help` cmdlet. For example:

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

Duplicate, enable or disable, rename, or delete an application

The following actions are available:

- **Duplicate:** You might want to duplicate an application to create a different version with different parameters or properties. When you duplicate an application, it is automatically renamed with a unique suffix and placed next to the original. You might also want to duplicate an application and then add it to a different group. (After duplicating, the easiest way to move an application is dragging it.)
- **Enable or disable:** Enabling and disabling an application is a different action than enabling and disabling a delivery group or application group.
- **Rename:** You can rename only one application at a time. If you try to rename an application and one with the same name exists in the same folder or group, you are prompted to specify a different name.
- **Delete:** Deleting an application removes it from the delivery groups and application groups with which it was associated, but not from the source that was used to add the application originally. Deleting an application is a different action than removing it from a delivery group or application group.

To duplicate, enable, disable, rename, or delete an application:

1. Select **Applications** in the left pane.
2. Select one or more applications and then select the appropriate task in the action bar.
3. Confirm the action, when prompted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remove applications from a delivery group

An application must be associated (belong) with at least one delivery group or application group. If you attempt to remove an application from a delivery group that would remove that application's association with any delivery group or application group, you are notified that the application will be deleted if you continue. When that happens, if you want to deliver that application, you must add it again from a valid source.

1. Select **Delivery Groups** in the left pane, and then select a delivery group.
2. On the **Applications** tab, select the application you want to remove.
3. Select **Remove from Delivery Group** from the action bar.
4. Confirm the removal.

Remove applications from an application group

An application must belong to at least one delivery group or application group. If you attempt to remove an application from an application group that will result in that application no longer belonging to any group, you are notified that the application will be deleted if you continue. When that happens, if you want to deliver that application, you must add it again from a valid source.

1. Select **Applications** in the left pane.
2. Select the application group, and then select one or more applications.
3. Select **Remove from Application Group** in the action bar.
4. Confirm the removal.

Pass parameters to published applications

Use the **Location** page of an application's properties to enter the command line and pass parameters to published applications.

When you associate a published application with file types, the symbols `"%*"` (percent and star symbols enclosed in double quotation marks) are appended to the end of the command line for the application. These symbols act as a placeholder for parameters passed to user devices.

If a published application does not launch when expected, verify that its command line contains the correct symbols. By default, parameters supplied by user devices are validated when the symbols `"%*"` are appended. For published applications that use customized parameters supplied by the user device, the symbols `"%**"` are appended to the command line to bypass command-line

© 1997–2026 Citrix Systems, Inc. All rights reserved.

validation. If you do not see these symbols in a command line for the application, add them manually.

If the path to the executable file includes directory names with spaces (such as `"C:\Program Files"`), enclose the command line for the application in double quotation marks to indicate that the space belongs in the command line. To do this, add double quotation marks around the path, and another set of double quotation marks around the `%*` symbols. Be sure to include a space between the closing quotation mark for the path and the opening quotation mark for the `%*` symbols.

For example, the command line for the published application Windows Media Player is:

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

NOTE:

The maximum number of characters, including arguments, in the command line for launching published applications is 203.

Troubleshooting session sign-out issues with Published Applications

When publishing applications, only the main executable file for the published application is specified. However, some applications might produce additional (child) processes that run in the background and are not closed by the corresponding main executable file when the main published application is closed. Additional processes might also be created, from scripts that are run, or from specific registry keys, like `Run` and `RunOnceKey`. These applications can prevent a graceful sign-out, resulting in lingering or hanging sessions and might result in the session not closing and the user being signed out.

In this case, you need to reset or exit these sessions using Citrix Director.

To help identify and troubleshoot sessions not being signed out properly, Citrix has made three registry entries available. Identifying and troubleshooting of session not being logged off properly due to these issues is a three-step process:

1. Identifying which sessions have published applications are holding up a graceful sign-out
2. Identifying for those published applications if they produce any additional (child) processes
3. Add these processes to a specified registry entry to prevent them from holding up sign-out

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Identifying for those published applications if they produce any additional (child) processes

Once a published application is identified to hold up a graceful sign-out, the next step is to determine if this application produces additional processes when running.

You can read `HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` to determine if any processes are blocking a graceful sign-out when a published application is closed.

In the following example, the key `LogoffCheckerBlockingProcess` contains the following entries:

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

These processes have held up the graceful sign-out.

NOTE:

Replace the with the correct session ID for the session you want to check.

Step 3: Add these processes to a specified registry entry to prevent them from holding up sign-out

You can add these processes to the following registry keys to prevent them from holding up sign-out in future sessions:

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

Type:REG_SZ
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
String:MyAppName.exe
```

More information about `LogoffCheckSysModules`, see Graceful logoff from a published application renders the session in an active state.

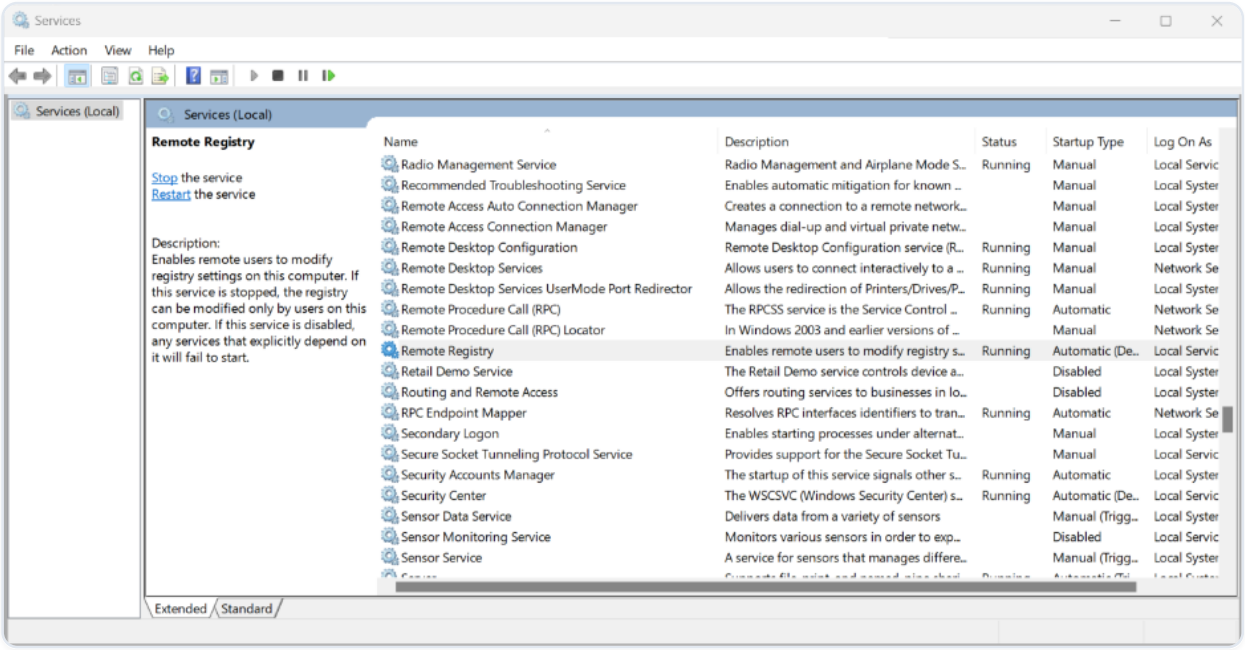
Step-by-step troubleshooting guide

1. Start the remote registry Service under the VDA under test:

   a. In the Control Panel, select **Administrative Tools > Services**.

   b. Right-click **Remote Registry Service** and select **Properties**.

   c. Under **Startup Type**, select **Automatic** from the drop-down menu.



2. Turn off the Windows Firewall on the VDA under test or create an inbound firewall rule to enable port 455:

   a. In the Control Panel, select **Windows Defender Firewall > Advanced Settings**.

   b. Right-click **Inbound Rules** and select **New Rule**.

   c. In **New Inbound Rule Wizard**, select **Port**.

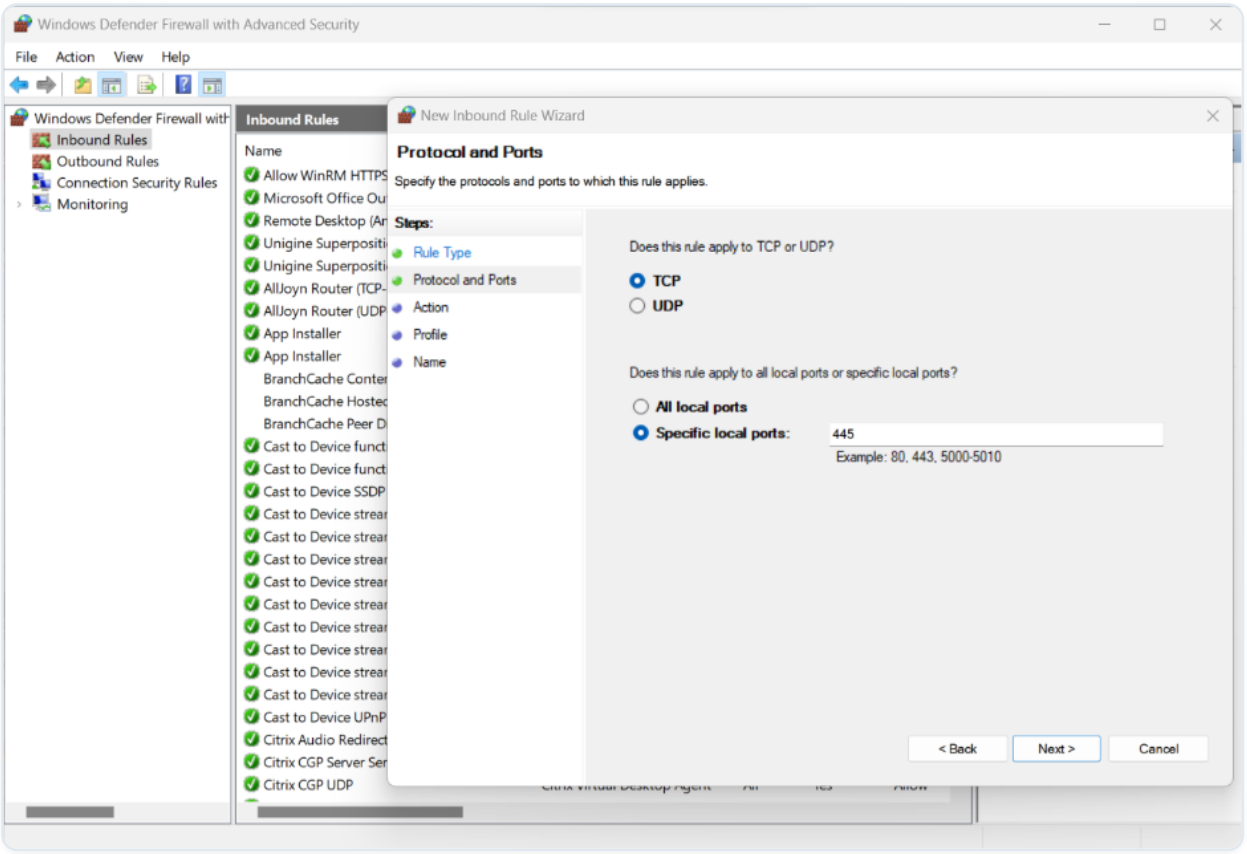
   d. On the **Protocols and Ports** page, select **TCP and Specific Local Ports**. Enter `445` as the local port.

   e. Select **Allow Connection** on the **Action** page.

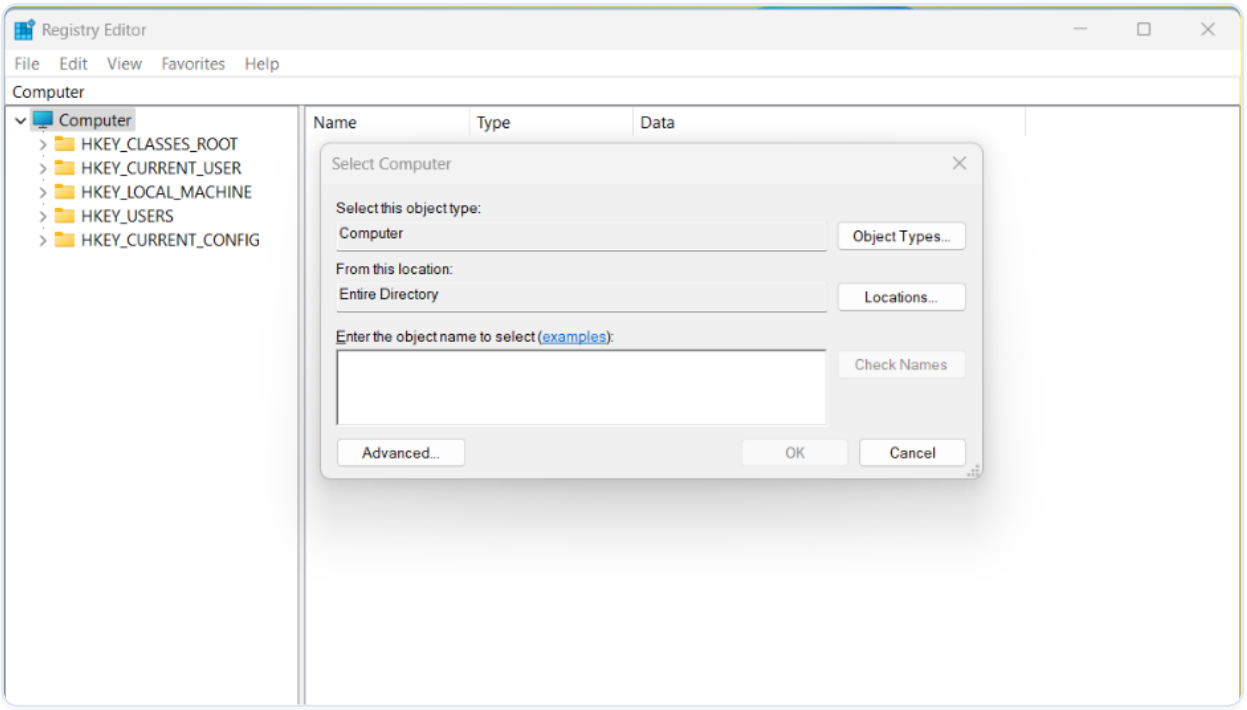
   f. Select the firewall profiles that you want to apply the new inbound rule.

   g. Name the firewall rule and select **Finish** to exit **New Inbound Rule wizard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

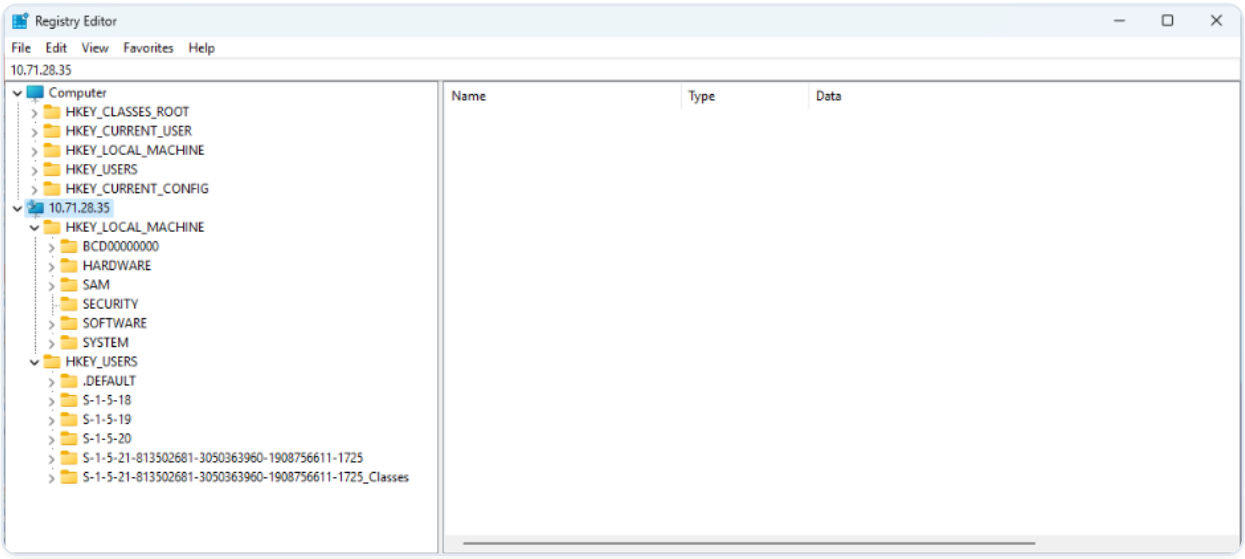


3. From another VM on the same domain (it can be DC, DDC, or another VDA), run `Regedit` and connect to a remote registry.

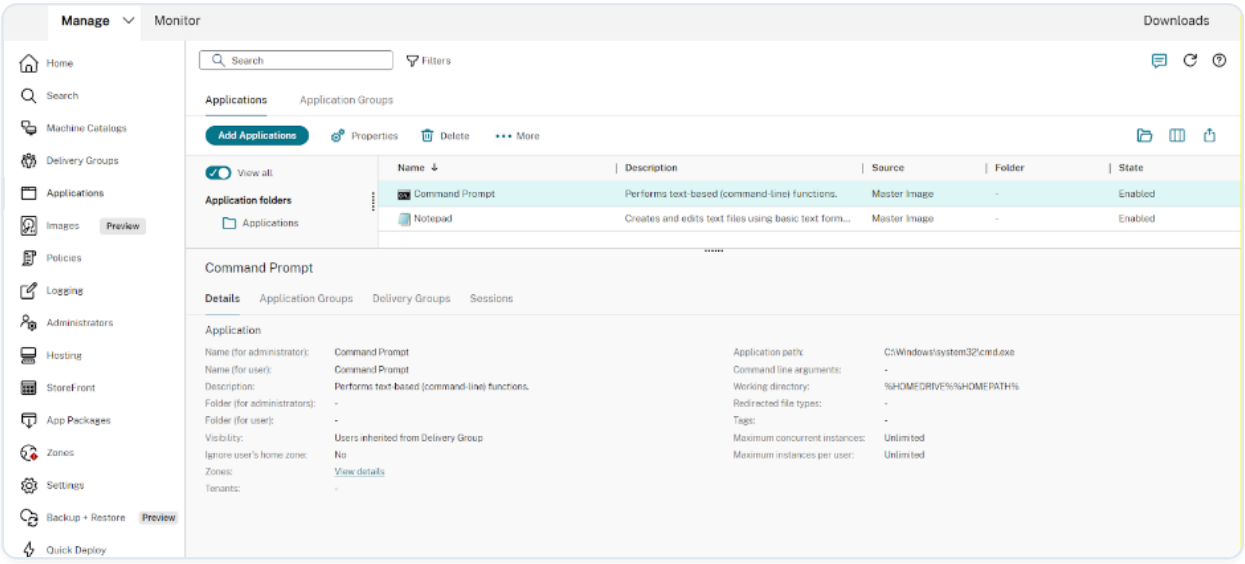


4. Enter the IP address of the VDA under test and click **OK**. The `regedit` tree must display branches for the VDA under test.

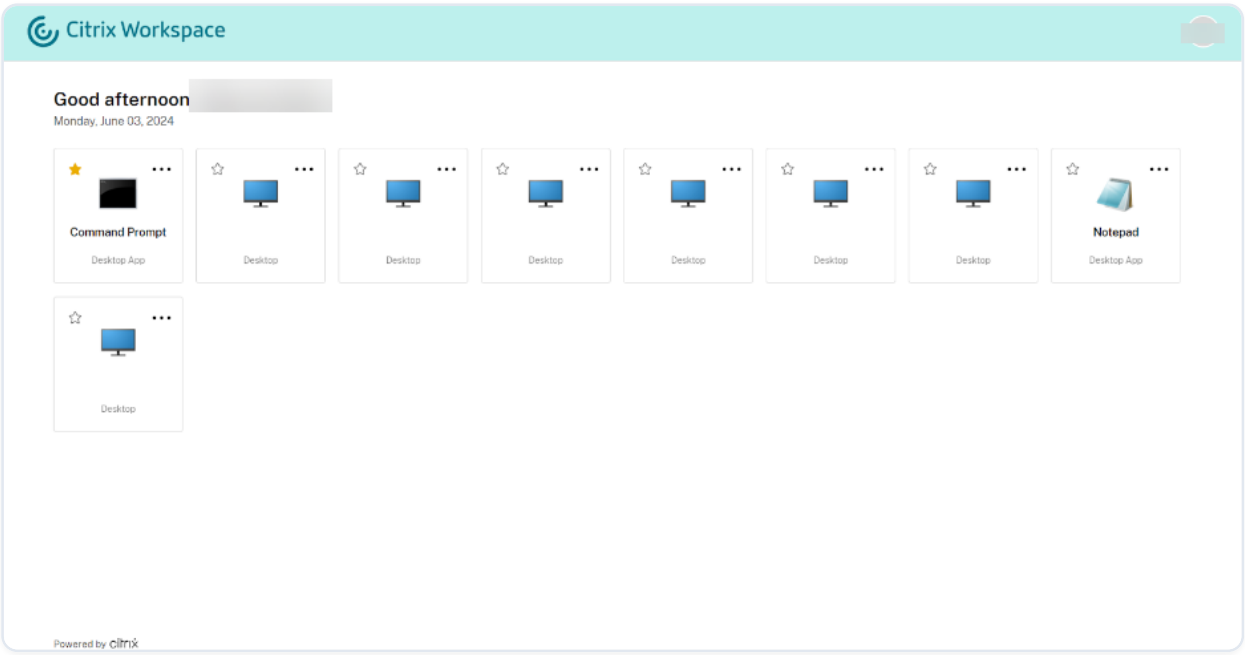
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Open the **Command Prompt** published application.

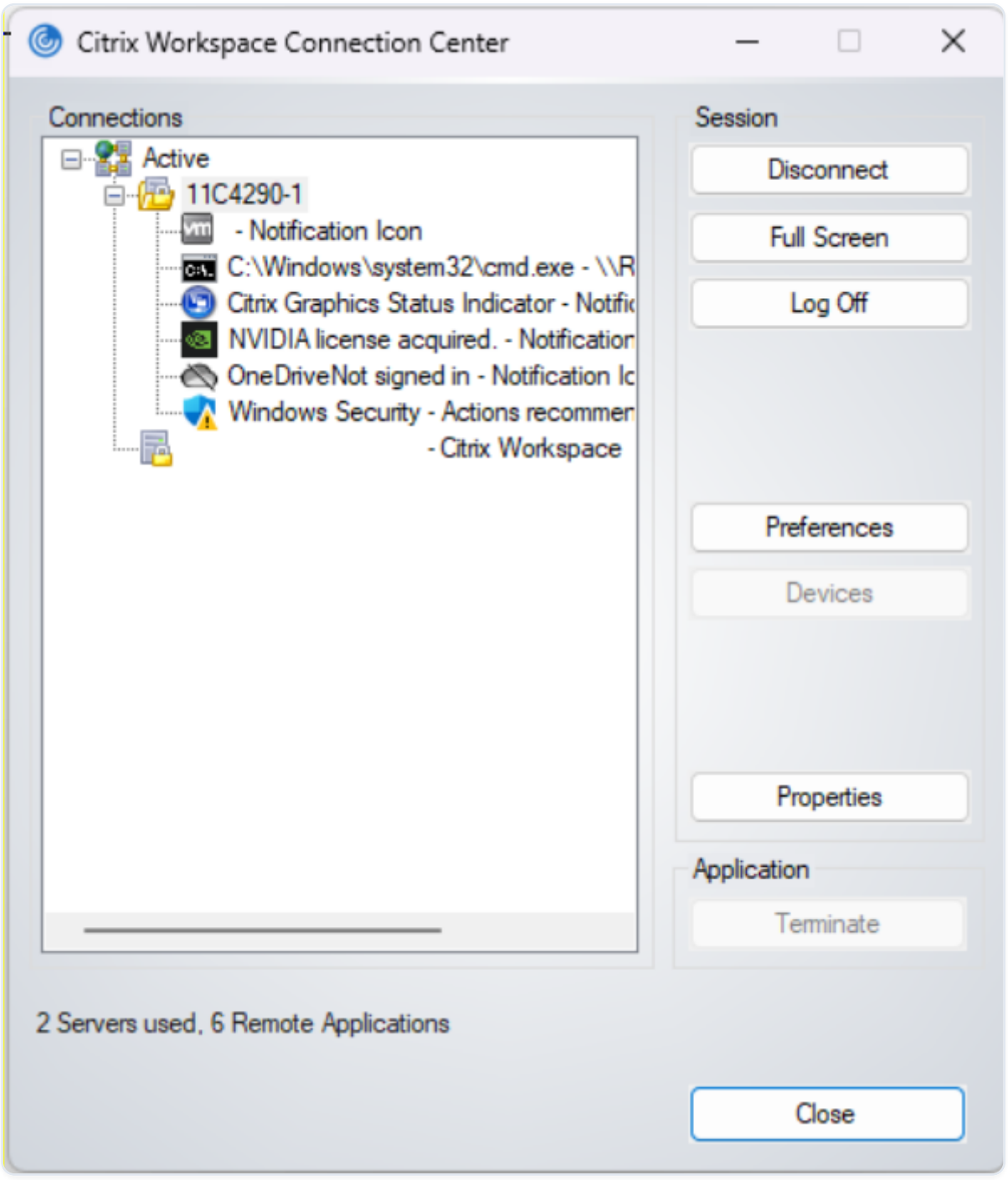


The **Command Prompt** app is displayed in Citrix Workspace app.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Open **Connection Center** on the client. This is used for monitoring when a session is signed out, after closing an opened seamless app. We can see in the following image that the Command Prompt process `c:\Windows\system32\cmd.exe` is active on the remote VDI.



7. From the VDA where **regedit** is running, go to the following remote IP location:
`HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

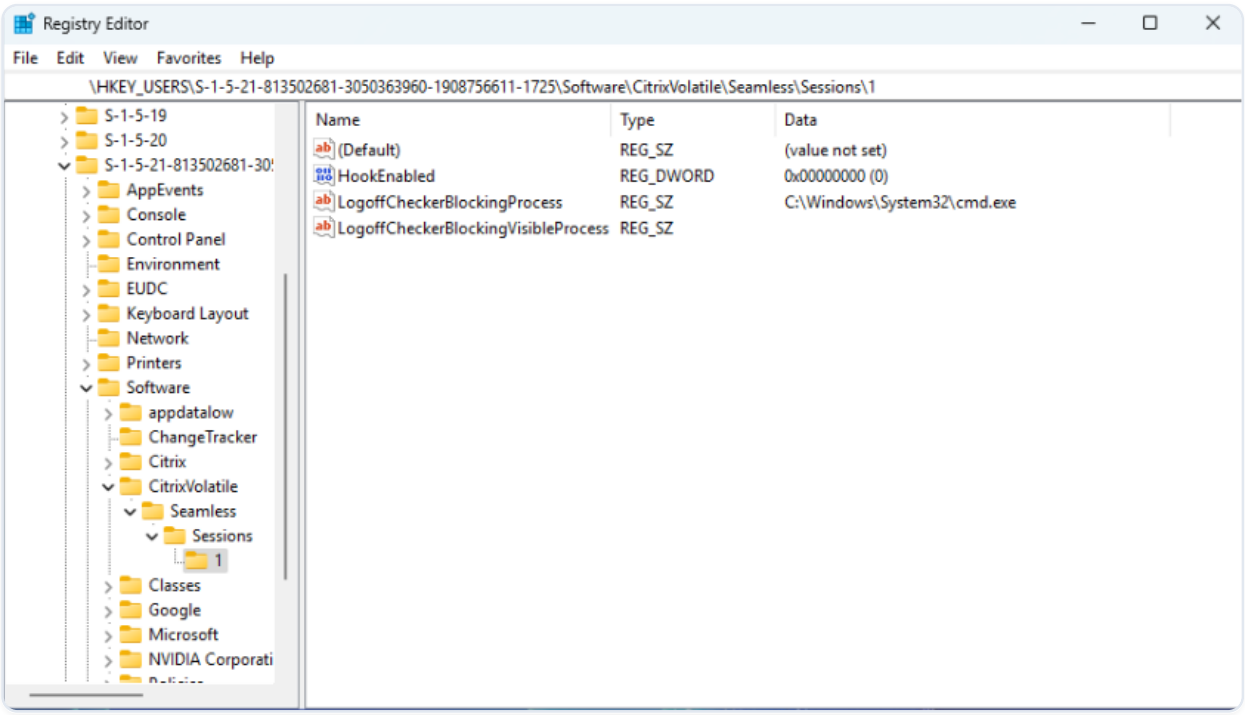
NOTE:

This path changes every time you open a new session.

8. There are two keys to read here (do not change them here): **LogoffCheckBlockingProcess** and **LogoffCheckerBlockingVisibleProcess**. These keys display any programs that are blocking sign-out. The first one must display `C:\Windows\System32\cmd.exe` since that was open and has not been closed yet.

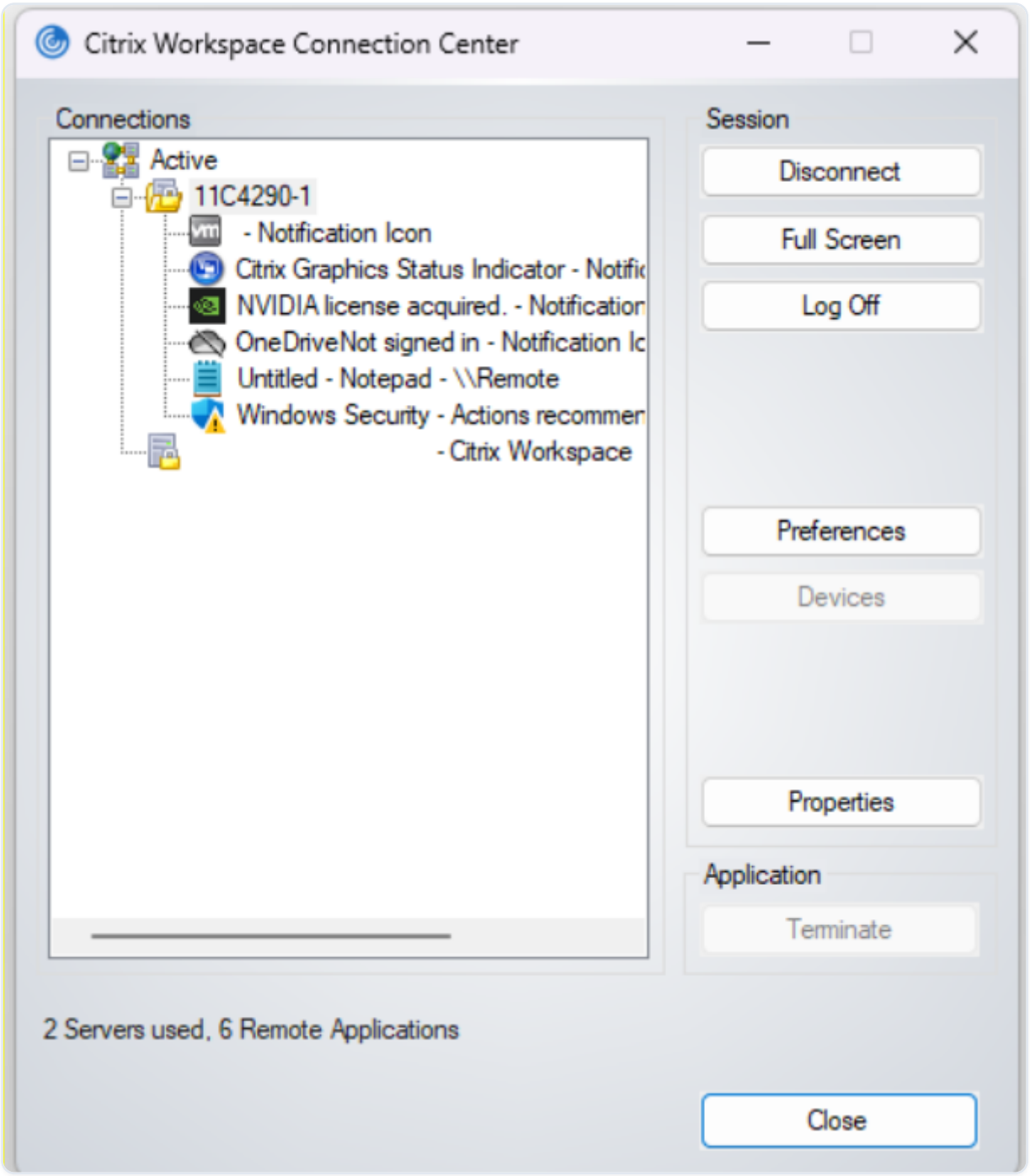
NOTE:

LogoffCheckBlockingProcess and **LogoffCheckerBlockingVisibleProcess** must not be manually edited. Manually editing these registry values can lead to unstable sessions.



9. Click **X** in the upper-right hand corner to exit **Seamless CMD**.
10. Check the connection center to see if the session closes. It may take up to 30 seconds to close. If it closes, there have been no applications or processes that have prevented a graceful sign-out.

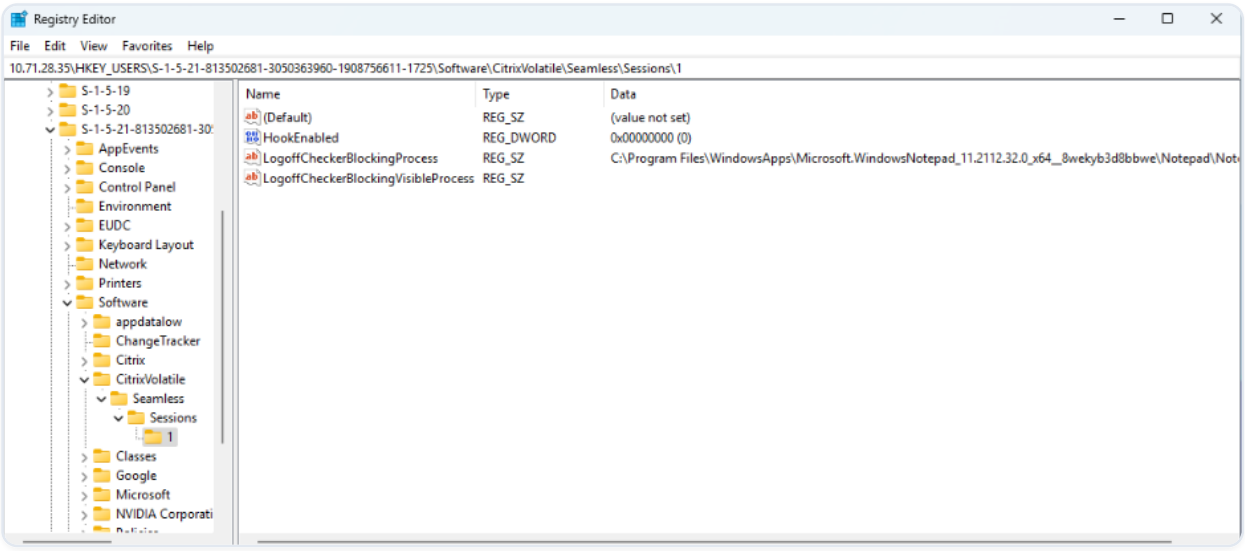
© 1997–2026 Citrix Systems, Inc. All rights reserved.



11. If the session did not close, refresh the **regedit** output with F5.
12. Check the contents of **LogoffCheckBlockingProcess** and **LogoffCheckerBlockingVisibleProcess** again. CMD must no longer be present but there should be another listed process. Whatever process is currently blocking session sign-out must be displayed here.

    In this case, **Notepad.exe** is open from the published command prompt before the command prompt was closed and this remote notepad process is holding up a graceful sign-out.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



13. Make a note of the path to this executable, and which key it appeared in, and enter it in the following registry key, under the remote tree:

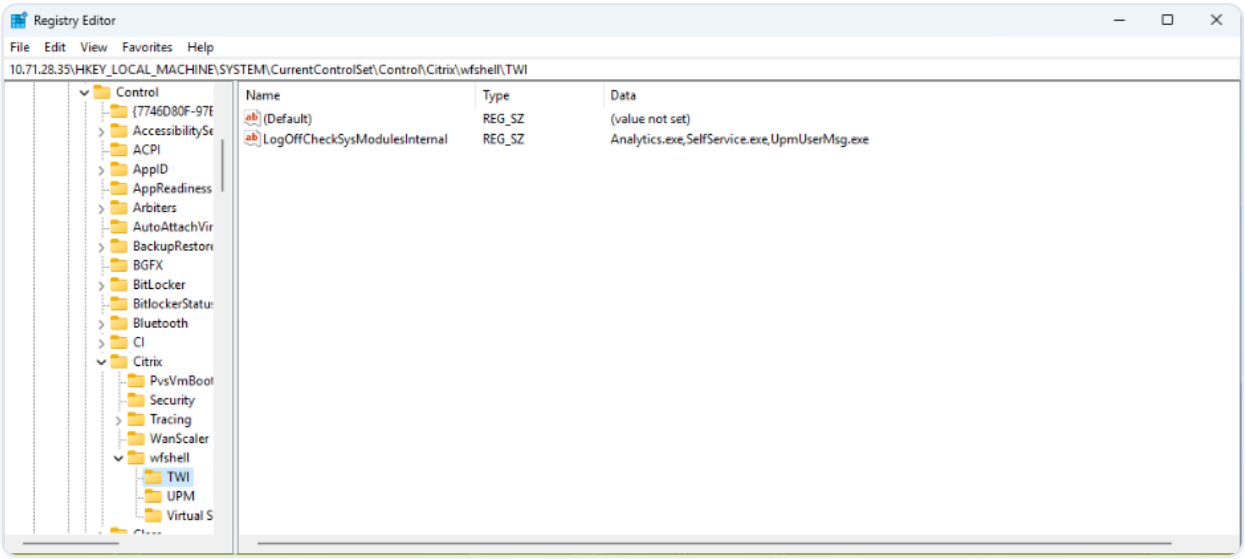
    - If it appears in **LogoffCheckBlockingProcess**:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - If it appears in **LogoffCheckerBlockingVisibleProcess**:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **NOTE:**
>
> If there is already one or more entries in the key, add a comma to the end and put the new entry after the comma.



14. Sign out from the session from the connection center on the client, and re-open the Remote Application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

15. Repeat steps 9-16 until the session is signed out automatically within 30 seconds of closing the Remote Application.

> **NOTE:**
>
> After troubleshooting, revert the temporary Firewall changes to allow remote registry access if needed.

How to modify LogonUI to view Windows disclaimer message in full size when opening published applications

The **LogonUI** window scaling is improved for scenarios where authentication pass-through does not occur. The **LogonUI** window is scaled based on the monitor resolution and DPI settings used which ensures that the complete **LogonUI** window is visible without any clipping.

The window size in pixels can also be set manually in the registry.

1. Open the **Registry Editor** using `regedit` on the **Run** command.
2. Go to `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`.
3. Create two new DWORD keys: **LogonUIWidth** and **LogonUIHeight**.
4. Set the value of the keys to the required width and height in pixels for the **LogonUI** window.

   When manually setting the **LogonUI** windows size, automatic scaling is disabled.

> **NOTE:**
>
> These registry paths have changed from 2407 and later. The old registry values are ignored and deprecated.

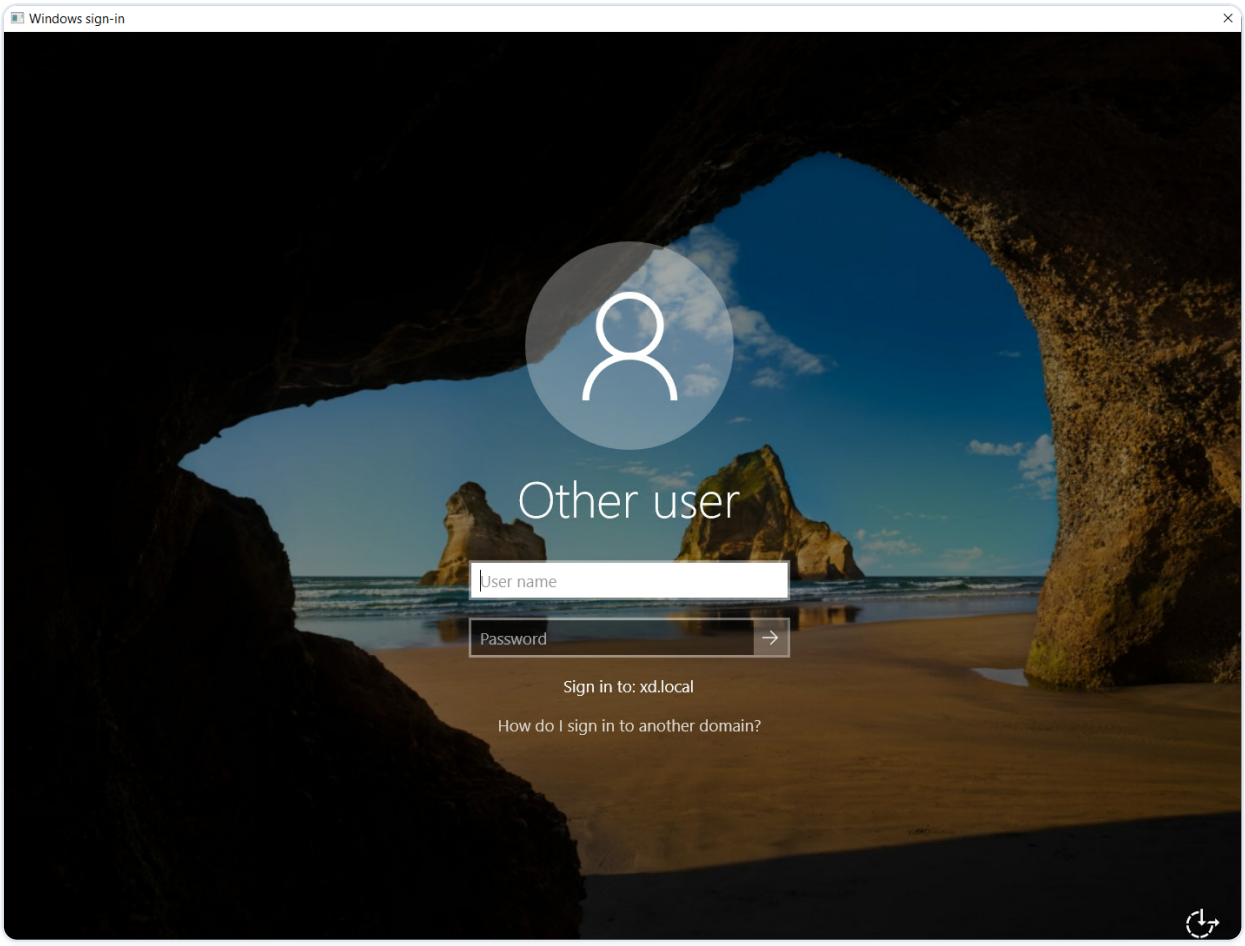
By default, the **LogonUI** window includes a title bar with a close button which enables the end user to disconnect from the session if needed.

Disable a tilebar

You can disable the tile bar in the **LogonUI** window with the following registry key:

1. Open the Registry Editor using `regedit` on the **Run** command.
2. Go to `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`.
3. Create new DWORD keys: **LogonUICaption** and set the value of the key to `0`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Manage application folders

By default, new applications you add to delivery groups are placed in a folder named **Applications**. You can specify a different folder when you create the delivery group, when you add an application, or later.

Good to know:

- You cannot rename or delete the Applications folder, but you can move all the applications it contains to other folders you create.
- A folder name can contain 1–64 characters. Spaces are permitted.
- Folders can be nested up to five levels.
- Folders do not have to contain applications. Empty folders are allowed.
- Folders are listed alphabetically in Web Studio unless you move them or specify a different location when you create them.
- You can have more than one folder with the same name, as long as each has a different parent folder. Similarly, you can have more than one application with the same name, as long as each is in a different folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You must have `View Applications` permission to see the applications in folders, and you must have `Edit Application Properties` permission for all applications in the folder to remove, rename, or delete a folder that contains applications.
- Most of the following procedures request actions using the action bar in Web Studio. Alternatively, you can use right-click menus or drag the item. For example, if you create or move a folder in a location you did not intend, you can drag/drop it to the correct location.
- All nodes in Studio (such as **Machine Catalogs**, **Delivery Groups**, **Applications**, and **Application Groups**) share the same folder tree in the back end. To avoid name conflicts when renaming or moving folders, use unique names for first-level folders across different nodes.

  If you create a folder using the `New-BrokerAdminFolder` SDK cmdlet and want it to appear under the **Applications** node, you must add the `ContainsApplications` metadata using the `Set-BrokerAdminFolderMetadata` cmdlet.

  Example:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

To manage application folders, select **Applications** in the left pane. Use the following list for guidance.

- **To view all folders (excluding nested folders):** Click **Show all** above the folder list.
- **To create a folder at the highest level (not nested):** Select the **Applications** folder. To place the new folder under an existing folder other than **Applications**, select that folder. Then, select **Create Folder** in the actions bar. Enter a name.
- **To move a folder:** Select the folder and then select **Move Folder** in the action bar. You can move only one folder at a time unless the folder contains nested folders. (The easiest way to move a folder is to drag it.)
- **To rename a folder:** Select the folder, and then select **Rename Folder** in the action bar. Enter a name.
- **To delete a folder:** Select the folder, and then select **Delete Folder** in the action bar. When you delete a folder that contains applications and other folders, those objects are also deleted. Deleting an application removes the application assignment from the delivery group. Tt does not remove it from the machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **To move applications into a folder:** Select one or more applications. Then, select **Move Application** in the action bar. Select the folder.

You can also place applications you are adding in a folder on the **Application** page when creating a delivery group or an application group. By default, added applications go in the **Applications** folder. Click **Change** to select or create a folder.

Control local launch of applications on published desktops

When users launch a published application from within a published desktop, you can control whether the application is launched in that desktop session or as a published application. Citrix Workspace app searches for the installation path of the application in the Windows registry on the VDA and, if present, launches the local instance of the application. Otherwise, a hosted instance of the application is launched. If you launch an application that is not installed on the VDA, the hosted application is launched. For more information, see vPrefer launch.

In PowerShell (using the Remote PowerShell SDK in Citrix Cloud deployments or the PowerShell SDK in on-premises deployments), you can change this action.

In the `New-Broker` Application or `Set-BrokerApplication` cmdlet, use the `LocalLaunchDisabled` option. For example:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

By default, this option's value is false (`-LocalLaunchDisabled $false`). When launching a published application from within a published desktop, the application is launched in that desktop session.

If you set the option's value to true (`-LocalLaunchDisabled $true`), the published application is launched. This creates a separate, additional session from the published desktop (using Citrix Workspace app for Windows) to the published application.

Requirements and limits:

- The application's `ApplicationType` value must be `HostedOnDesktop`.
- This option is available only through the appropriate PowerShell SDK. It is not currently available in the Web Studio graphical interface.
- This option requires minimum: StoreFront 3.14, Citrix Receiver for Windows 4.11, and Delivery Controller 7.17.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App packages

App packages are pre-configured application deployments that Citrix® manages. They allow applications to be virtualized, which implies that the applications run independently of the user's device's operating system and interface.

App packages simplify application management, reduces IT overhead, and ensures that applications are secure and functional throughout their lifecycle.

Citrix supports the following packaging technologies for delivering applications to users:

- App-V applications
- MSIX and MSIX app attach applications
- FlexApp applications
- Elastic App applications
- Cloudpaging applications

This article walks you through how to deploy and deliver these packaged applications in your Citrix DaaS™ environment.

App-V applications

Application Virtualization (App-V) is a Microsoft technology that allows applications to be streamed and accessed without requiring installation on the end user's device. Citrix DaaS can use App-V to deliver applications, providing a centralized and efficient way to manage applications across various client machines.

For more information about the components and concepts with which you interact when delivering App-V packaged applications, see the Microsoft documentation: Application Virtualization (App-V) for Windows client overview.

Important terms

- **Management server**: Provides a centralized console to manage App-V infrastructure and delivers virtual applications to both the App-V Desktop Client and a Remote Desktop Services Client. The App-V management server authenticates, requests, and provides the security, metering, monitoring, and data gathering required by the administrator. The server uses Active Directory and supporting tools to manage users and applications.
- **Publishing server**: Provides App-V clients with applications for specific users, and hosts the virtual application package for streaming. It fetches the packages from the management server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Dynamic configuration files**: App-V packages can be customized using dynamic configuration files, that when applied to the package, can be used to change its characteristics. For example, you can use them to define extra application shortcuts and behaviors. For more information, see Dynamic configuration files

Dynamic configuration files

Citrix App-V supports both types of dynamic configuration files. File settings are applied when the application is launched:

- **Deployment Configuration files** provide machine-wide configuration for all users. These files are expected to be named `<packageFileName>_DeploymentConfig.xml` and in the same folder as the App-V package they apply to. These files are supported by single and dual admin management.
- **User Configuration files** provide user-specific configuration that supports per-user customizations to the package. Single Admin supports user config files named in the following format: `<packageFileName>_[UserSID | Username | GroupSID | GroupName_]UserConfig.xml` and located in the same folder as the App-V package they apply to.

  When multiple User Configuration files exist for a particular package, they are applied with the following priority:

  a. User SID
  b. Username
  c. AD Group SID (First found wins)
  d. AD Group Name (First found wins)
  e. Default

  For example:

  ```
  MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

  MyAppVPackage_joeblogs_UserConfig.xml

  MyAppVPackage_S-1-5-32-547_UserConfig.xml

  MyAppVPackage_Power Users_UserConfig.xml
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
MyAppVPackage_UserConfig.xml
```

NOTE:

The user-specific portion of the file name can also optionally occur at the end (for example `MyAppVPackage_UserConfig_joeblogs.xml`).

IMPORTANT:

You cannot apply changes to Dynamic Deployment Configuration when there are user sessions with an application in the package open. You can apply changes to Dynamic User Configuration files if other users (but not the current user) have the application from the package open.

Dynamic configuration file location

In single admin management, the Citrix App-V components only process dynamic configuration files, which are found in the same folder as their App-V package.

When applications in the package are launched, any changes to the corresponding dynamic configuration files are reapplied. If your dynamic configuration files are in a different location to their packages, use a mapping file to map packages to their deployment configuration files.

To create a mapping file:

1. Open a new text file.
2. For each dynamic configuration file, add a line that specifies the path to the package using the format `<PackageGuid> : path`.

   For example:

   ```
   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
   ```

3. Save the file as `ctxAppVDynamicConfigurations.cfg` in the same folder as the package.

The entire directory hierarchy on the same UNC share as the App-V package is searched recursively upwards for this file every time an application in the package is launched.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Methods

You can use the following methods to deliver and manage App-V packages:

- **Dual Admin**: In this method, Citrix DaaS and App-V servers work together to deliver and manage packages. This method requires Citrix DaaS to periodically refresh the snapshot view of the App-V server's state. It incurs hardware, infrastructure, and administration overhead. Citrix DaaS and App-V servers must stay synchronized, particularly for user permissions.

  This method works best in closely coupled App-V and Citrix deployments. In this method:

  - **App-V management server** handles the dynamic configuration files
  - **App Packages Delivery Component** installed on VDA machines: Manages the registration of the appropriate publishing server required for an application launch.

  This ensures that the publishing server is synchronized for the user at the appropriate time. The publishing server maintains other aspects of the app package life cycle (like refresh on logon and connection groups) using the settings that it is configured with.

- **Single Admin**: Application packages are stored on network shares. Citrix DaaS delivers and manages packages independently.

  This method reduces overhead because the App-V servers and database infrastructure aren't needed in the deployment.

  In this method, you store App-V packages on a network share and upload their metadata from that location to your environment. The App Packages Delivery Component installed on VDA machines then manages and delivers applications as follows:

  - Process the Deployment Configuration Files and User Configuration Files when an application is launched.
  - Manage all aspects of the life cycles for packages on the host machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- You can use one or both management methods simultaneously. In other words, when you add applications to Delivery Groups, the applications can come from App-V packages located on App-V servers or on a network share.
- If you are using both management methods simultaneously, and the App-V package has a dynamic configuration file in both locations, the file in the App-V server (dual management) is used.
- When you select App packages in the Web Studio navigation pane, the display shows package names and profiles. The **Package type** column indicates which technology is used to deliver the package and where they are referenced in the **Application Library**. When you select a package, the details pane lists the applications and shortcuts in the package.

MSIX and MSIX app attach applications

MSIX is a Windows app package format that provides a modern packaging experience to all Windows apps. MSIX is suitable for various Windows application types, including Win32, .NET, and UWP apps.

MSIX app attach utilizes MSIX packages that are pre-expanded onto virtual hard disks, which can be mounted to the target machine as required, rather than streaming the package contents. It can improve deployment times, reduce network traffic, and lower IOPS on the target machine, but requires additional work to create and maintain the app attach disks.

Citrix DaaS delivers MSIX and MSIX app attach applications to users through the **App Packages Delivery Component** installed on VDA machines. This component manages all aspects of the life cycles for packages on the host machine.

For more information about MSIX and MSIX app attach, see the Microsoft documentation: MSIX documentation and App Attach in Azure Virtual Desktop respectively.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- We support native MSIX Packages on Desktop and server VDAs and MSIX app attach on `.vhd`, `.vhd` and `.cim` disk image formats on Desktop VDAs only.
- Microsoft does not offer an AppAttach implementation for Server 2019. While AppAttach is present in Server 2022 and 2025, Microsoft does not support it on these versions. Therefore, we also do not support AppAttach on Server 2022 and 2025.
- Enable sideloading on Windows Server 2019.
- Ensure VDAs trust the certificates that packages are signed with.

FlexApp applications

FlexApp is an application layering solution developed by Liquidware that attaches any application to a Windows session without modifying the underlying base image through the traditional application installation process.

FlexApp One applications are encapsulated in a single, shareable file, allowing them to operate without requiring an additional application layer on Windows sessions. Users can initiate the application by clicking the container file, which quickly integrates one or more applications into their Windows workspace.

Citrix delivers FlexApp applications to users through the App Packages Delivery Component and FlexApp delivery agent installed on VDA machines. These two components manage all aspects of the life cycles for packages on the host machine.

Elastic App applications

Elastic App technology is a feature of Citrix App Layering that lets you assign application layers to users dynamically at logon, rather than installing them into a base image. With Elastic App technology, applications follow the user across different virtual machines, ensuring that they always have access to the apps they need without bloating the master image.

Citrix DaaS delivers Elastic App applications to users through the Citrix Personalization component and Application Layering Enterprise Layer Manager (ELM). These two components manage all aspects of the life cycles for packages on the host machine. For more information about Application Layering Enterprise Layer Manager, see the Citrix App Layering™ document.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cloudpaging applications

Cloudpaging is Numecent's application streaming technology that delivers applications to a Windows session without requiring changes to the base image.

With Cloudpaging, applications launch almost instantly because only a small portion of the code (typically less than 10%) is streamed initially. The remaining components stream in the background when users access them, providing a seamless experience.

For Citrix environments, the App Packages Delivery Component on the VDA works with the Numecent Cloudpaging Player to manage the application lifecycle. The Citrix component orchestrates delivery, while the Cloudpaging Player handles on-demand streaming and execution within the session.

Configuration requirements

Consider the following configuration details:

CLOUDPAGING PLAYER AND LOGOFFCHECKSYSMODULES

When using virtual published applications with Cloudpaging containers, configure the following settings to allow a session to log off:

SETTING	VALUE
Registry Key	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`
Value Name	`LogoffCheckSysModules`
Value Type	`REG_SZ`
Value Data	`CoreHelper.exe`

URLS FOR WHITELISTING

In addition to the standard URL whitelisting requirements, VDAs require access to the following endpoint:

PARAMETER	VALUE
URL	`external-api.cloudpager.net`
Port	443

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	VALUE
Client	Cloudpager PowerShell Module
Forward Proxy Config for Web-Based	• Outbound access allowed • Authentication bypass required
Description	Cloudpager PowerShell Module

Optionally, you can create a dedicated delivery group with a VDA used solely to perform Cloudpager discovery to limit required whitelisted URLs. We recommend creating a delivery group with a machine that has **VDA version 2511 or later** and **App Packages Delivery Component** installed.

For more information about Cloudpager Client network and firewall requirements, see the Numecent knowledgebase article.

Deploy and deliver app packages

Prerequisites

To support the delivery of App-V, MSIX, MSIX app attach, FlexApp packages, Elastic App, and Cloudpaging applications, you must first install the **App Packages Delivery Component** on VDA machines. See Install the App Packages Delivery Component on VDA machines for details.

INSTALL THE APP PACKAGES DELIVERY COMPONENT ON VDA MACHINES

The App Packages Delivery Component manages the publishing process for application packages in App-V, MSIX, MSIX app attach, FlexApp, Elastic App, and Cloudpaging formats. This component isn't installed by default when you install a VDA. You can install the component during or after VDA installation.

To install the component during VDA installation, use either of the following ways:

- In the installation wizard, go to the **Additional Components** page and then select the **App Packages Delivery Component** checkbox.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In the command line interface, use the `/includeadditional "Citrix Personalization for App-V – VDA"` option.

To install the component after VDA installation, follow these steps:

1. On the VDA machine, go to **Control Panel > Programs > Programs and Features**, right-click **Citrix Virtual Delivery Agent**, and then select **Change**.
2. In the wizard that appears, proceed to the **Additional Components** page and then enable the **App Packages Delivery Component** checkbox.

NOTE:

- Microsoft App-V Desktop Client is the component that runs virtual applications from App-V packages on user devices. Windows 10 (1607 or later), and Windows Server 2019 and later already include this App-V client software. You must only enable it on VDA machines. For more information, see this Microsoft documentation article: Enable the App-V in-box client.
- For FlexApp applications, install the FlexApp One Agent on the VDA along with the App Packages Delivery Component.
- For Elastic App applications, install the App Layering-enabled image on the VDA along with the App Packages Delivery Component.
- For Cloudpaging applications, install the Cloudpaging Player on the VDA along with the App Packages Delivery Component.

INSTALL THE FLEXAPP ONE AGENT

1. Launch an administrator command prompt on the VDA.
2. Locate the network path for any FlexApp One Package.
3. Input the following command:

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. Accept any prompts that appear.

INSTALL THE APP LAYERING-ENABLED IMAGE

1. Set up app layering. Follow the instructions in the Citrix App Layering documentation. The process includes:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Set up the Enterprise Layer Manager (ELM).
b. Import a gold OS image.
c. Create a platform layer.
d. Create application layers.
e. In ELM, select the **Enable this App Layer for use with Studio App Packages** checkbox for each application layer you want to deliver.

2. Install an image including the Elastic Layering component on VDA machines. You can use one of the following ways:

a. Deploy the image from ELM with Elastic Layering enabled.
b. Install the VDA manually on the machine and select the Elastic Layering component during setup.

INSTALL THE CLOUDPAGING PLAYER

1. Open an administrator command prompt on the VDA.
2. Go to the folder that contains the Cloudpaging Player installer.
3. Run the following command to install the player silently and configure the SaaS console URL. Replace the placeholder values as needed:

```
cloudpaging-player-setup-x64-release.exe /S /v"/qn ADDLOCAL=ALL
REG_BASETOKENPATHORURL=https://your-tenant-url/api/token"
```

4. (Optional) Verify the configuration after installation by checking the following registry value:

- **Path:** `HKEY_LOCAL_MACHINE\SOFTWARE\Numecent\StreamingCore\Settings\Launcher`
- **Name:** `BaseTokenPathOrURL`
- **Data:** The value must match the URL you specified during installation.

Deliver packaged applications

After you complete installing the prerequisites, do the following to deliver packages applications to your users:

1. Store application packages on network shares.
2. Upload application packages into your environment.
3. Add applications to delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. To enable automatic delivery of interdependent App-V packages, create isolation groups.

STORE APPLICATION PACKAGES ON NETWORK SHARES

After you set up the infrastructure, generate the application packages and store them in a network location, such as a UNC or SMB network share, or on an Azure File Share.

Detailed steps are as follows:

1. Generate application packages. See the Microsoft documentation: Creating and managing App-V virtualized applications for details.
2. Store application packages in a network location:
   - For **App-V Single Admin**: Store the packages and the corresponding Dynamic Configuration Files (App-V) on a UNC or SMB network share or on an Azure File Share.
   - For **App-V Dual Admin**: Publish the packages onto the App-V management server from a UNC path. (Publishing from HTTP URLs isn't supported.)
   - For **MSIX or MSIX app attach**: Store the packages on a UNC or SMB network share or on an Azure File Share.
   - For **FlexApp**: Store the packages on a UNC or SMB network share or an Azure File Share.
   - For **Elastic App**: Store the packages on a UNC or SMB network share or an Azure File Share.
   - For **Cloudpaging**: Store the packages on a UNC or SMB network share or an Azure File Share.
3. Make sure that the VDA has read permission on the package storage path:
   - If you store packages on a UNC or SMB network share in your AD domain, grant the VDA machine read permission to the storage path. To do so, you can give the machine's AD account read permission to the share explicitly, or include the account in an AD group that has that permission.
   - If you store packages on an Azure File Share, first grant a user account read permission to the storage path in Azure. Next, configure `ctxAppVService` running on the VDA machine to use that user account to access the package storage path. See the Change the user logon account for the detailed steps.

CHANGE THE USER LOGON ACCOUNT

Change the user logon account in the following two scenarios:

- To access packages on an Azure File Share using a linked AD account:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - The connecting entity must be a user account, not a machine account, as Microsoft Entra ID doesn't grant read permissions to machine accounts on File Shares.

- If MSIX and MSIX AppAttach packages contain services:

    - The package must be published using a user account with administrative privileges on the local machine before it can be published to any non-administrative users. This is necessary for packaged services to be installed and packages can only be published to users, not machines, making the default LocalService account unsuitable.

The VDA calls `ctxAppVService` to access package storage paths and perform operations that require administrative privileges. By default, `ctxAppVService` runs under the context of the machine's LocalService account that authenticates to AD using the machine's identity and is not suitable for the preceding scenarios.

In either case, the service must be reconfigured to use an AD user account that has administrative privileges locally and has been granted read access to the storage location for the packages, be that an SMB share or an Azure File Share, as follows:

1. Start **Services**, right-click **ctxAppVService**, and then select **Properties**.
2. On the **Log on** tab, select **This account**:
    a. Enter a user account that has local administrative privileges and read permission to the package storage path
    b. Enter the user's password twice.
3. Click **OK**.

UPLOAD APPLICATION PACKAGES INTO YOUR ENVIRONMENT

After you store application packages to a network location as needed, upload them to your environment for delivery. Use either of the following methods as needed:

- Upload in bulk
- Upload one by one

Preparations
Citrix DaaS uses a VDA machine to set up the connection to the network location for package discovery. Therefore, create a delivery group beforehand and make sure that at least one VDA in the group meets the following requirements:

- VDA version:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - To discover App-V packages: 2203 or later
    - To discover MSIX and MSIX app attach packages: 2209 or later
    - To discover FlexApp packages: 2311 or later and the FlexApp Agent software
    - To discover Elastic App packages: 2511 or later and the App Layering-enabled image
    - To discover Cloudpaging packages from the Cloudpager console: 2511 or later
    - To discover Cloudpaging packages from a network share: 2603 or later

- App Packages Delivery Component: Installed
- Permission on the package location: Read (See Store application packages on network shares for details.)
- Power: On
- State: Registered

Upload application packages in bulk
Upload packages in a network location to your environment. Make sure that you have the following items ready before the upload:

- A delivery group that meets the Preparations requirements
- The network location path

To upload packages in bulk, follow these steps:

1. In the left pane, select **App packages**.
2. On the **Package discovery** tab, click the **Create discovery profile** button. The **Create discovery profile** page appears.
3. In the **Name** field, enter a descriptive name for the profile.
4. In the **Delivery group** field, click **Select a delivery group**. Next, select a delivery group that meets the requirements stated in Preparations and then click **OK**.
5. In the **Location type** field, select **Microsoft App-V server**, **Network share**, or **Numecent Cloudpager** based on where you store the packages, and then complete the corresponding settings:

    - If you selected **Microsoft App-V server**, enter the following information:

        - URL of the Management server. Example: `http://appv-server.example.com`
        - Login credentials of the management server administrator.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - URL and port number of the publishing server. Example: `http://appv-server.example.com:3330`

- If you selected **Network share**, specify the following information:
    - Enter the UNC path of the network share (Example: `\\Package-Server\apps\`). For *Elastic App packages*, enter the UNC path from the **System's Network File Share SMB path** in ELM.
    - Select the package types that you want to upload. Options include **App-V**, **MSIX**, **MSIX app attach**, **FlexApp**, **Elastic App**, and **Cloudpaging**.
    - Specify whether to search subfolders for packages.

      NOTE:

      If you search for MSIX app attach packages on a folder structure containing `cim` images, ensure that you select the **Search** subfolders. Otherwise, the disks are not discovered correctly.

- If you selected **Numecent Cloudpager** (which means Cloudpaging apps are stored in the Cloudpager console), enter the following information:
    - Cloudpager console URL. Example: `https://cloudpagerconsole.my.org`
    - PowerShell API key.
    - AppLauncher MSID.

6. In the **Preferences** section, configure the following options as needed:
    - **Remove absent packages**: Select this option to automatically remove packages from the **Packages** tab if they are no longer found in the profile location during update checks. If not selected, such packages appear with a disabled icon.
    - **Upgrade in place**: Select this option to overwrite an existing package with a newer version discovered during an update check. When selected, user favorites are retained after the upgrade. This option is selected by default.
    - **Ignore downgrade**: Select this option to skip importing a package if a higher version of the same package already exists in the library. This option is selected by default.
7. Click **Create discovery profile**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Create discovery profile** page closes and the newly added profile appears in the profile list. Citrix DaaS uploads the packages to Citrix Cloud using a VDA in the delivery group. After the upload completes, the Status field shows Import successful. The corresponding packages appear on the **Packages** tab.

NOTE:

- To check for package updates in a profile location and import them to Citrix Cloud, select the location in the profile list and click **Check for Updates**.
- When you select a discovery profile in the list, the details pane shows the current values of **Upgrade in place** and **Ignore downgrade** as **Yes** or **No**.
- When you click **Check for Updates**, the confirmation panel also displays the current **Upgrade in place** and **Ignore downgrade** settings before the check runs.

Upload application packages one by one

Upload an application package from a network share to your environment. Before the upload, make sure that you have the following items ready:

- A delivery group that meets the requirements stated in Preparations
- The network location path.

To upload a package to your environment, follow these steps:

1. In the left pane, select **App Packages**.
2. On the **Packages** tab, click the **Add Package** button. The **Add Package** page appears.
3. In the **Delivery group** field, click **Select a delivery group**. Next, select a delivery group that meets the requirements stated in Preparations, and then click **OK**.
4. In the **Package full path** field, enter a path as needed:
   - To upload several packages at a time, enter their full paths, separated by semicolons (`;`). Example: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - To upload all packages present on a network share, enter the storage path. Example: `\\package-Server\apps\`
5. In the **Preferences** section, configure the following options as needed:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Upgrade in place**: Select this option to overwrite an existing package with a newer version when one is found. When selected, user favorites are retained after the upgrade. This option is selected by default.
- **Ignore downgrade**: Select this option to skip importing this package if a higher version of the same package already exists in the library. This option is selected by default.

6. Click **Add Package**.

The application package appears on the **Packages** tab.

ADD APPLICATIONS TO DELIVERY GROUPS

After an application package is fully uploaded to your environment, add its applications to one or more delivery groups as needed. As a result, users associated with those delivery groups can access the applications.

NOTE:

- You can deliver packaged applications to single-session VDAs and multi-session VDAs through delivery groups.
- By default, end users have access to all packaged applications assigned to the delivery groups associated with their *single-session* (or called *Desktop*) VDAs. To limit visibility of a packaged application on *desktop* VDAs to specific users or groups, go to the **Applications** node, select the application, and then select **Edit Application Properties > Limit Visibility** to make changes. See Limit visibility of applications

To add one or more applications in a package to several delivery groups, follow these steps:

1. In the left pane, select **App Packages**.
2. On the **Packages** tab, select a package as needed.
3. In the action bar, click **Add Delivery Groups**. The **Assign Applications to Delivery Groups** page appears.
4. Select where to deliver applications from this app package, select one or more applications in the package for the Citrix Workspace app, and then click **Next**.

- **Deliver the app package on the desktop**: All applications in this package are delivered on Citrix virtual desktops. End users can access them by launching a desktop from their store's **Desktops** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Deliver the applications on Citrix Workspace**: Selected applications in this package are delivered as Citrix virtual apps. End users can access them from their store's **Apps** tab.

> **NOTE:**
>
> This setting controls the default visibility of packaged applications. To change the visibility of a specific packaged application later, go to the **Applications** node, select the application, and choose **Properties > Delivery** to make changes. For more information, see Change application properties.

5. In the list of delivery groups, select the groups to which you want to assign the applications, and then click **Next**.

> **NOTE:**
>
> - If you selected an MSIX or MSIX app attach package, only delivery groups whose VDA version is 2106 or later are shown in the list.
> - If you selected a *FlexApp* package, only delivery groups whose VDA version is 2402 or later appear in the list.
> - If you selected an *Elastic App* package, only delivery groups whose VDA version is 2511 or later appear in the list.
> - If you selected a *Cloudpaging* package, only delivery groups whose VDA version is 2511 or later appear in the list.

6. Click **Finish**.

To add applications in various packages to multiple delivery groups, follow these steps:

1. In the left pane, select **App Packages**.
2. On the **Applications** tab, select **Add Applications**.
3. On the **Groups** page, select one or more delivery groups as needed.
4. On the **Applications** page, select one or more application packages as follows:
    a. Click **Add** and then select **Application packages**.
    b. Select the type of package needed (for example, App-V Single Admin). All packages of this type appear.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Select one or more packages as needed.

d. Click **OK** and then **Next**.

e. To add more applications of a different package type, repeat steps a through d.

5. Click **Finish**.

You can also add packaged applications to a delivery group when:

- Creating a delivery group. For more information, see Create delivery groups.
- Editing existing delivery groups or application groups. For more information, see Add applications.

(OPTIONAL) CREATE ISOLATION GROUPS FOR APP-V PACKAGES

You can create isolation groups to enable the automatic delivery of interdependent App-V packages.

NOTE:

Isolation groups are supported for the App-V Single Admin method. If you're using the App-V Dual Admin method, you can achieve the same goal by creating *connection groups* in the Microsoft App-V infrastructure. For more information, see this Microsoft documentation article: About the connection group file.

About isolation groups

An isolation group is a collection of interdependent application packages that must run in the same Windows Sandbox to create a virtual environment. Citrix App-V isolation groups are similar but not identical to App-V connection groups. An isolation group includes two types of packages:

- **Explicit application packages**: Applications with specific licensing requirements. You can restrict those applications to a specific range of users by adding them to delivery groups.
- **Automatic application packages**: Applications that are always available to all users regardless of whether they are added to delivery groups.

For example, the application `app-a` requires JRE 1.7 to run. You can create an isolation group that contains app-a (marked as *Explicit*) and JRE 1.7 (marked as *Automatic*). Next, add the App-V package for `app-a` to one or more delivery groups. When a user launches app-a, JRE 1.7 is automatically deployed with it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When a user starts an App-V application marked as *Explicit* in an isolation group, Citrix DaaS checks the user's access permission to the application in delivery groups. If the user has permission to access the application, any *Automatic* application packages in the same isolation group are made available to the user.

You do not need to add the *Automatic* packages to any delivery group. If there's another *Explicit* application package in the isolation group, that package is made available to the user only if it is in the same delivery group.

Create an App-V isolation group

Create an isolation group and add interdependent application packages to it. Detailed steps are as follows:

1. On the **Isolation Groups** tab, click **Add Isolation Group**.
2. Enter a name and description for the isolation group. All App-V Single Admin packages in your environment appear in the **Available Packages** list.
3. From the **Available Packages** list, select an application as needed, and then click the right arrow. The selected application appears in the **Packages in Isolation Group** list.
4. In the **Deployment** field, select **Explicit** or **Automatic** for the application.
5. Repeat steps 2–3 to add more packages.
6. To adjust the order of packages in the list, click the up or down arrow.
7. Click **Save**.

NOTE:

Isolation Group configurations result in the creation of an App-V Connection Groups on the VDA. Deployment scenarios can become complex and the App-V client supports packages that are only in one active Connection Group at a time. We recommend that you avoid adding the same package to two different isolation groups that are added to the same delivery group.

Best practices

- To deploy App-V packages, enable the App-V subsystem on the VDA using the PowerShell command `Enable-AppV`.
- To deploy MSIX (and AppAttach) packages, the VDA must trust the certificates that the packages are signed with.
- On Windows Server 2019, enable sideloading to deploy MSIX packages. Sideloading is not needed for Windows 10, 11, Windows Server 2022, and 2025.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- App Attach has no implementation at all on Windows Server 2019 and is not currently supported by Microsoft (or Citrix by extension) on Windows Server 2022 or 2025.

Advanced

The following advanced topics provide additional configuration options and controls to fine-tune how packaged applications are discovered, updated, and delivered in Citrix DaaS beyond the basic app package workflow.

Automate packaged application publishing

You can use PowerShell commands to automate packaged application publishing:

On the Delivery Controller™, run the following PowerShell commands:

1. To load the commands present in the Package Discovery Module:

   ```
   Import-Module "D:
   \Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
   ```

   NOTE:

   The version of the package discovery module can be found on the Citrix DaaS ISO on the path mentioned in step 1.

2. The package discovery module must be from the ISO of a Citrix DaaS version that also supports the package type you are publishing, that is, 2311 or higher is needed for FlexAppOne Applications. We recommend using the latest available.
3. To retrieve the relevant delivery group IDs and packaged application IDs:

   ```
   Get-BrokerDesktopGroup | Format-Table Uid, Name

   Get-AppLibAppVApplication | Format-Table Uid, Name
   ```

4. To publish the packages and create the appropriate BrokerMachineConfigurations:

   ```
   Publish-PackagedApplication -AppLibararyApplicationUid
   <AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
   ```

5. To synchronize the Broker configurations, which are later sent out to the Broker agent on VDA:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid
<DesktopGroup.Uid>
```

NOTE:

Ensure to run the PowerShell command `Update-DesktopGroupMachineConfigurations` after you publish or remove packaged applications from a delivery group through the PowerShell command line. Otherwise information about the published applications is not sent to the VDA correctly and launches fail.

Limit visibility of applications

In a Citrix DaaS environment, when applications from packages are published to desktops, the system respects Active Directory (AD) user and group visibility settings for those applications. However, even if a user only has visibility to one application within a package, the entire package must be deployed to the Virtual Desktop (or Seamless App) Session since individual package components cannot be subdivided on the VDA. Additionally, before VDA version 2503, changes that reduce application visibility after the initial publishing won't result in a clean-up of previously published packages on subsequent desktop launches. Furthermore, other visibility layers, such as desktop versus workspace visibility, operate on top of these AD visibility assignments.

You can control whether packaged applications must appear in Workspace or are deployed to the users' VDI Desktop sessions. Once a packaged application has been published you can update the `PackagedApplicationVisibility` property on the `BrokerApplictaion` using the PowerShell command `Set-BrokerApplication -Name "MyApp" -PackagedApplicationVisibility "Workspace|Desktop|WorkspaceAndDesktop"`.

The default value of `PackagedApplicationVisibility` is `WorkspaceAndDesktop`.

The value `Workspace`: app appears only in WorkspaceApp and is available for a seamless AppLaunch, but the app won't automatically be published to any desktop session that users start.

The value `Desktop`: hides the app's icon from WorkspaceApp making it unavailable for a seamless AppLaunch but the app can still be deployed to users' desktop sessions if users also have access to it through their AD Group settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Packaged Applications published to Single Session Static desktops are never available in Workspace App regardless of the value configured in this setting.

Migrate from App-V full infrastructure to Single Admin workflow

Microsoft App-V full infrastructure (Dual Admin) is approaching the end of life. To continue delivering App-V packages and other supported container formats, migrate to the Citrix Single Admin model.

The Single Admin model removes the dependency on the App-V Management and Publishing servers and centralizes package management in Studio.

Benefits of Single Admin model

Moving to the Single Admin workflow simplifies your architecture and streamlines package management.

SIMPLIFIED ARCHITECTURE

In the Single Admin model, the VDA retrieves packages directly from the file share. Citrix manages metadata, publishing, and isolation logic.

FEATURE	FULL INFRASTRUCTURE (DUAL ADMIN)	SINGLE ADMIN (CITRIX MANAGED)
Management	App-V Management Console	Citrix Studio or Web Studio
Database	Required (SQL Server)	None (metadata stored in the Citrix site database)
Publishing	App-V Publishing Server	Citrix VDA (`ctxAppVService`)
Package source	UNC share (synchronized to Management Server)	UNC share, SMB share, or Azure Files
Logic	Connection Groups	Citrix Isolation Groups

STRATEGIC ADVANTAGE

By moving to Single Admin, you also eliminate the **Synchronization Lag**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In the Dual Admin model, you must synchronize the App-V Management Server, and then synchronize Studio.
- In the Single Admin model, when you update a package on the file share and select **Refresh** in Studio, the updated package is available at the next user logon.

Migration workflow

Follow these steps to move your existing App-V full infrastructure to the Citrix Single Admin workflow:

1. Step 1: Prepare the target environment
2. Step 2: Import packages into the Citrix library

STEP 1: PREPARE THE TARGET ENVIRONMENT

Before importing packages, ensure that your infrastructure and VDAs are ready to support the Single Admin model.

1. **Shared repository**
   a. Identify the UNC share that hosts your `.appv` packages.
   b. Ensure that VDA machine accounts (for example, Domain Computers) have **Read** access to both the share and NTFS permissions.
2. **VDAs**

   Ensure that all VDAs have the **App Packages Delivery Component** installed. To add this component after installation:

   a. Run the VDA installer.
   b. Select **Change** in **Programs and Features**.
   c. Add **App Packages Delivery Component**.
3. **XML configuration files**

   Move the `_DeploymentConfig.xml` and `_UserConfig.xml` files into the *same* folder as the corresponding `.appv` file.

   In the Single Admin model, the VDA reads configuration files from the package folder on the file share instead of from a central App-V database.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STEP 2: IMPORT PACKAGES INTO THE CITRIX LIBRARY

After you prepare the environment, import your existing App-V packages into the Citrix application library.

1. In Citrix Studio, go to **Configuration** > **App Packages**.
2. If you are fully migrating, remove any existing connections to the App-V Management Server.
3. Select **Add Package** and point it to the UNC path of your package.
4. Citrix scans the folder and imports package names, versions, and application IDs into the Citrix application library.

After import, you can assign applications to delivery groups as needed.

NOTE:

vPrefer Policy (Optional): If you want applications to launch on the local VDA instead of redirecting to a remote server, enable the **vPrefer** GPO on your VDAs.

Troubleshoot App-V applications (Single Admin model)

If App-V packages (in the Single Admin model) fail to launch or don't appear in the user session, use the following guidance to identify and resolve common issues.

ISSUE	DESCRIPTION	SOLUTION
Package discovery and "Failed to catalog" errors	When you add a package in Studio, an error indicates that the file cannot be accessed or that the metadata is invalid.	1. Verify permissions. Ensure that the Delivery Controller machine account (for example, `DOMAIN\DDC01$`) has **Read** permissions on both the share and NTFS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE	DESCRIPTION	SOLUTION	
		levels of the UNC path that hosts the package. 2. Check XML integrity. Ensure that the `.appv` file and the `_DeploymentConfig.xml` file have the same file name prefix and are located in the same folder.	
Application fails to launch (error code: 0x80070005 or 0x80040154)	The user clicks the application icon and the **Citrix splash** screen appears, but the application does not open.	1. Verify the VDA component. Ensure that the **App Packages Delivery Component** is installed on the VDA. Confirm that the following file exists: `C:\Program Files\Citrix\AppV\ctxAppVService.exe`.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE	DESCRIPTION	SOLUTION
		2. Check VDA permissions. Because the VDA pulls the package from the file share, the VDA machine account (for example, `DOMAIN\VDA-HR01$`) must have **Read** access to the UNC path. 3. Validate the App-V client configuration. • Run the following PowerShell command on the VDA: `Get-AppvClientConfiguration`. • If your package requires scripts, ensure that `EnablePackageScripts` is set to `$True`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE	DESCRIPTION	SOLUTION
Isolation group conflicts	A plug-in, such as an Excel add-in, cannot see its parent application.	1. In Studio, go to **App Packages** > **Isolation Groups**. 2. Ensure that both packages are added to the same isolation group. In the Single Admin model, the App-V client on the VDA manages the virtual connection of those applications based on the configuration delivered by the Delivery Controller.
Slow initial launch (buffering)	The first launch of a large App-V package, such as AutoCAD or ArcGIS, takes several minutes.	1. On the VDA, check the following registry: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AppV`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE	DESCRIPTION	SOLUTION	
		`\Client\Streaming` 2. Set `Autoload` to `2` (auto-load all previously used packages) to improve subsequent launch performance. 3. Check network performance. Ensure that SMB signing or antivirus scanning on the network share isn't limiting transfer speed.	

Useful PowerShell commands (run on the VDA)

To verify whether Citrix successfully delivered the package to the VDA, run the following commands in a PowerShell window:

COMMAND	PURPOSE
`Get-AppvClientPackage`	Displays all App-V packages currently cached or published to the VDA.
`Get-CtxAppvPackage`	Displays the packages managed by the Citrix agent.
`Start-Service ctxAppVService`	Restarts the Citrix App-V orchestration service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Autoscale™

Autoscale provides a consistent, high-performance solution to proactively power manage your machines. It aims to balance costs and user experience. Autoscale incorporates the deprecated Smart Scale technology into Studio's power management solution.

Autoscale enables proactive power management of all registered single-session and multi-session OS machines in a delivery group.

Autoscale features include:

- Schedule-based and load-based settings
- Dynamic session timeouts
- Autoscale tagged machines (cloud burst)
- Dynamic machine provisioning
- User logoff notifications

Typical use cases

The following are the scenarios where AutoScale is commonly used.

- Scheduled-based machine powering on to handle expected workload

  Autoscale allows admins to vary the powered-on capacity with 30 min granularity and allows for different schedules on different days. If a volatile workload is expected, it is advised to configure the capacity buffer to avoid users having to wait for machines to power on.

- Cloud burst use case

  Autoscale provides the flexibility to power manage only a subset of machines in a delivery group. To achieve this, apply a tag to one or more machines and then configure Autoscale to power manage only tagged machines.

  This feature can be useful in cloud bursting use cases, where you want to use on-premises resources (or reserved public cloud instances) to handle workloads before cloud-based resources address additional demand (that is, burst workloads).

- Users ramping up slowly or seasonal users

  When an organization has users onboarding slowly and does not want to provision the entire capacity ahead of time, then the dynamic provisioning feature can help. The feature constantly evaluates the load on the delivery group and dynamically scale up or down the number of

© 1997–2026 Citrix Systems, Inc. All rights reserved.

machines in the delivery group based on the current load conditions. An admin must define the high and low watermark for the load on the delivery group to create machines. Admins can optionally define the maximum number of machines to be provisioned and tags to be applied to these machines.

Supported VDA hosting platforms

Autoscale supports all the platforms that Citrix DaaS supports. This includes various infrastructure platforms including XenServer (formerly Citrix Hypervisor), AWS, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere, and many more. For a complete list of supported platforms, see System requirements for Citrix DaaS.

Supported workloads

Autoscale supports both multi-session OS and single-session OS delivery groups. There are three user interfaces to be aware of:

- Autoscale user interface for multi-session OS delivery groups (formerly RDS delivery groups)
- Autoscale user interface for single-session OS random (pooled) delivery groups (formerly pooled VDI delivery groups)
- Autoscale user interface for single-session OS static delivery groups (formerly static VDI delivery groups)

For more information about the user interfaces for different delivery groups, see Autoscale user interfaces.

Benefits

The Autoscale feature delivers the following benefits:

- Provide you with a single, consistent mechanism to power manage machines in a delivery group.
- Ensure availability and control costs by powering machines with load-based or schedule-based power management, or a combination of both.
- To monitor metrics such as cost savings and capacity utilization, and to enable notifications, use Director, available on the **Monitor** console.

Watch a 2-minute video

The following video provides a quick tour of Autoscale.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Get started with Autoscale™

Autoscale is a feature that provides a consistent, high-performance power management solution to proactively scale delivery groups based on a configured schedule or load demands.

Autoscale applies to all types of delivery groups:

- Single-session static OS
- Single-session random OS
- Multi-session random OS

This article describes basic Autoscale-related concepts and provides guidance on how to enable and configure Autoscale for a delivery group.

Basic concepts

Before you start, learn about the following basic concepts in Autoscale:

- Capacity and machine registration
- Scale across multiple machine catalogs
- Machine provisioning and session demand
- Instance size considerations
- Schedules
- Peak and Off-Peak times
- Power-Off delay
- Pool size
- Capacity buffer
- Load index
- Autoscale and maintenance mode
- Machine cost
- Scale up a delivery group
- Scale down a Delivery Group
- Drain state

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Capacity and machine registration

Autoscale includes only machines that are registered with the site when determining the capacity. Powered-on machines that are unregistered can't accept session requests. As a result, they aren't included in the overall capacity of the delivery group.

Scale across multiple machine catalogs

In some sites, multiple machine catalogs might be associated with a single delivery group. Autoscale randomly powers on machines from each catalog to meet schedule or session demand requirements.

For example, a delivery group has two machine catalogs: Catalog A has three machines powered on and Catalog B has one machine powered on. If Autoscale needs to power on an extra machine, it might power on a machine from either Catalog A or Catalog B.

Machine provisioning and session demand

The machine catalog associated with the delivery group must have enough machines to power on and off as demand increases and decreases. If session demand exceeds the total number of registered machines in the delivery group, Autoscale ensures that all registered machines are powered on. However, **Autoscale does not provision additional machines**.

NOTE:

If a Delivery Group has 63 machines and a buffer capacity of 10% is set for off-business hours, then as per the Autoscale calculation, 6.3 machines must be turned on during off-business hours. To handle the decimal value, the following are the rules:

- Round to nearest: For example, if the value is 6.4, then 6 machines are turned on. If the value is 6.7, then 7 machines are turned on.
- Round to 1 for any non-zero value less than 1. For example, if the value is 0.2 or 0.9, then 1 machine is turned on.

To overcome this bottleneck, you can use a PowerShell script to create machines and delete them dynamically. For more information, see Dynamically provision machines

Instance size considerations

You can optimize your costs if you appropriately size your instances in public clouds. We recommend that you provision smaller instances as long as they match your workload performance and capacity requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Smaller instances host fewer user sessions than larger instances. Therefore, Autoscale puts machines into drain state faster because it takes less time for the last user session to be logged off. As a result, Autoscale powers off smaller instances sooner that reducing costs.

Schedules

Autoscale powers on and off machines in a delivery group based on a schedule that you set.

A schedule includes the number of active machines for each time slot, with peak and off-peak times defined.

Schedule settings vary with the type of delivery group. For more information, see:

- Multi-session OS delivery groups
- Single-session OS random delivery groups
- Single-session OS static delivery groups

Peak and off-peak times

Peak and off-peak times are used to indicate which of the capacity buffer values to use for specific periods of the day. You can define the peak times, leaving the remaining undefined times as off-peak times.

Power-Off delay

Power-off delay is the minimum number of minutes that must elapse after a machine is powered on before Autoscale can power off that machine. This keeps machines from flip-flopping on and off during volatile session demands. By default, the power-off delay is 30 minutes. You can set it in a range of 0-60 minutes.

Pool size

Pool size is the number of machines that must be kept powered-on for a particular period of a day.

Capacity buffer

Capacity buffer is used to add spare capacity to the current demand to account for dynamic load increases. There are two scenarios to be aware of:

- For multi-session OS delivery groups, the capacity buffer is defined as a percentage of the total capacity of the delivery group in terms of load index.
- For single-session OS delivery groups, the capacity buffer is defined as a percentage of the total number of machines in the delivery group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The capacity buffer is a rolling buffer, given that it is calculated and applied based on the current usage rather than calculated and applied on top of the configured pool size.

For example, given a delivery group with 10 machines, a pool size of 1 machine for the current period and a capacity buffer of 10%. An additional machine is powered on when the 1 powered-on machine, as defined by the schedule, is loaded to the point where the 10% capacity buffer is no longer satisfied. If the load is reduced after powering on the second machine and there is more than enough free load capacity to satisfy the 10% capacity buffer, Autoscale prepares 1 machine for power off.

Load index

IMPORTANT:

The load index applies only to multi-session delivery groups.

The load index metric determines how likely a machine is to receive user logon requests. It's calculated using the **Citrix Load Management policy** settings configured for concurrent logon, session, CPU, disk, and memory use.

The load index ranges from 0 to 10,000. By default, a machine is considered at full load when it's hosting 250 sessions:

- The digit "0" indicates an unloaded machine. A machine with a load index value of 0 is at a baseline load.
- The digit "10,000" indicates a fully loaded machine that can't run any more sessions.

Autoscale and maintenance mode

Machines in maintenance mode, regardless of their availability status, are considered as part of the calculation of the overall pool size. Therefore, it's possible for all machines within the pool to be in maintenance mode. However, these machines are excluded from the capacity buffer calculations, ensuring their immediate availability. To guarantee a specific percentage of machines are accessible for user connections, adjust the pool size and buffer values accordingly.

Machine cost

Machine instance cost per hour is the cost per hour, in US$, of the computing capacity being used. This setting is used to calculate the cost savings of the Autoscale settings. To view the savings, go to **Monitor > Cost Optimization > Cost savings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scale up a delivery group

Autoscale powers on additional machines in an Autoscale-enabled delivery group when:

1. The Autoscale schedule for the delivery group indicates that more machines must be powered on for the current time period.
2. The current load on the delivery group has exceeded the capacity buffer.

Conditions for powering on machines:

1. Not in maintenance mode.
2. Hypervisor is not in maintenance mode.
3. Powered off and unregistered.
4. Belongs to the delivery group that requires scaling up
5. No pending power actions.

Scale down a delivery group

Autoscale powers off machines in an Autoscale-enabled delivery group when:

1. The Autoscale schedule specifies that machines must be powered off to meet the configured number of machines for the current time period.
2. The current load of the delivery group has decreased, resulting in more powered-on machines than required to meet the pool size and capacity buffer.

Autoscale scales down a delivery group by powering off the excess machines exceeding the number needed to meet the pool size and capacity buffer.

The scale-down process involves two steps:

1. Place the required number of machines into the drain state.
2. Select all drained machines for power off.

Machines eligible for power off must meet the following criteria:

1. Not in maintenance mode
2. Hypervisor not in maintenance mode
3. Currently powered-on
4. Registered as available or is waiting to register after starting up
5. Drained and has no active sessions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. No pending power actions
7. Satisfies the power-off delay

Drain state

Autoscale attempts to scale down the number of powered-on machines in the delivery group to the configured pool size and capacity buffer.

To achieve this goal, Autoscale puts the excess machines with the fewest sessions into "drain state" and powers them off when all sessions are logged off. This behavior occurs when session demand lessens and the schedule requires fewer machines than are powered on.

Conditions for the machines to drain:

1. Powered-on
2. Not be in maintenance mode
3. Hypervisor not in maintenance mode
4. Belongs to the delivery group that requires scaling down
5. Least number of current active sessions

NOTE:

- Machines that have been on for at least the time specified by the Power-Off delay are preferred for drain.
- Machines in drain state no longer host new session launches and waits for the existing sessions to be logged off. A machine is shut down only when all sessions are logged off. However, if there are no machines immediately available for session launches, Autoscale prefers directing the session launches to a machine in drain state over powering on a machine.

Autoscale puts excess machines into "drain state" one by one:

- If two or more machines have the same number of active sessions, Autoscale drains the machine that has been powered on for the specified power-off delay.

  Doing so avoids putting recently powered-on machines into drain state because those machines are more likely to have the fewest sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If two or more machines have been powered on for the specified power-off delay, Autoscale drains those machines one by one at random.

Machines in drain state no longer host new session launches and are waiting for the existing sessions to be logged off. A machine becomes a candidate for shutdown only when all sessions are logged off. However, if there are no machines immediately available for session launches, Autoscale prefers directing the session launches to a machine in drain state over powering on a machine.

A machine is taken out of drain state when one of the following conditions is met:

- The machine is powered off.
- Autoscale is disabled for the delivery group to which the machine belongs.
- Autoscale uses the machine to meet schedule or load demand requirements. This case occurs when the schedule (schedule-based scaling) or the current demand (load-based scaling) requires more machines than the number of machines that are currently powered on.

IMPORTANT:

If no machines are immediately available for session launches, Autoscale prefers directing session launches to a machine in a drain state over powering on a machine. A machine in a drain state that hosts a session launch remains in drain state.

To find out which machines are in drain state, use the `Get-BrokerMachine` PowerShell command. For example: `Get-BrokerMachine -DrainingUntilShutdown $true`. Alternatively, you can use Studio. See Display machines in drain state.

DISPLAY MACHINES IN DRAIN STATE

NOTE:

This feature applies only to multi-session machines.

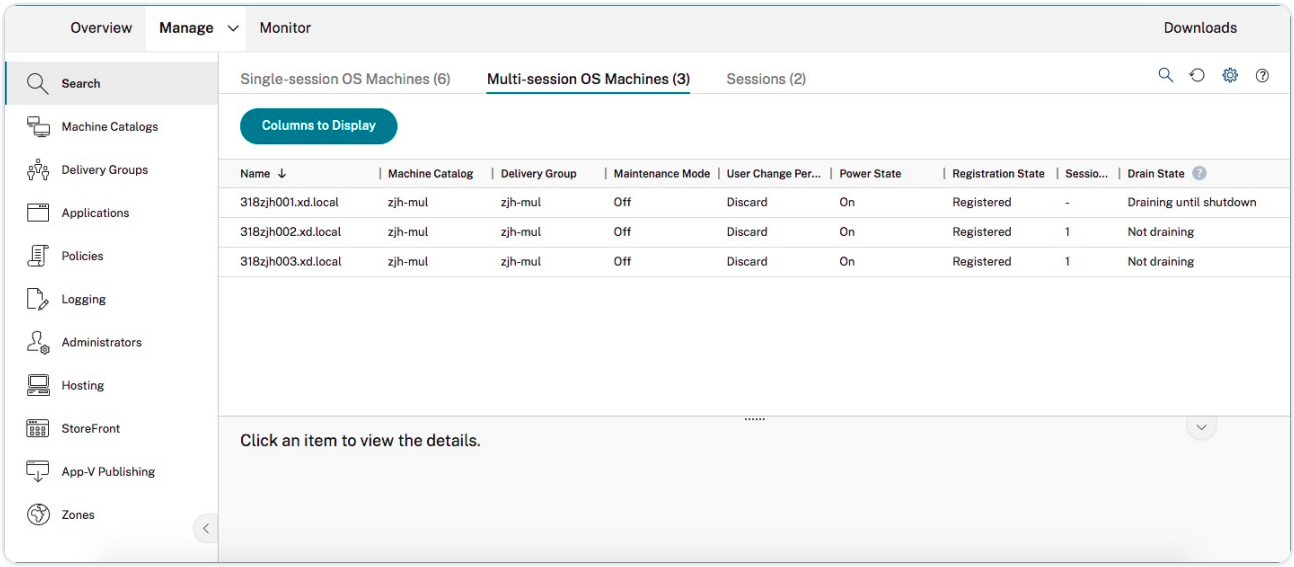
In Studio, you can display machines that are in drain state, letting you know which machines are about to shut down. Complete the following steps:

1. Navigate to the **Search** node and then click **Columns to Display**.
2. In the **Columns to Display** window, select the checkbox next to **Drain State**.
3. Click **Save** to exit the **Columns to Display** window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Drain State** column can display the following information:

- **Draining until shutdown.** Appears when machines are in drain state until they're shut down.
- **Not draining.** Appears when machines aren't yet in a drain state.

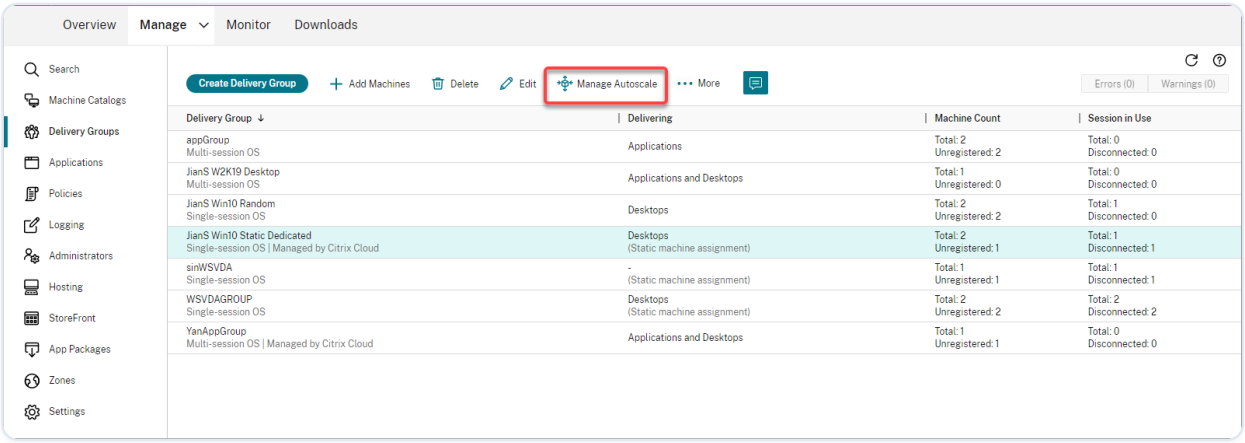


Enable Autoscale for a delivery group

Autoscale is disabled by default when you create a delivery group. To enable and configure Autoscale for a delivery group using Studio, follow these steps:

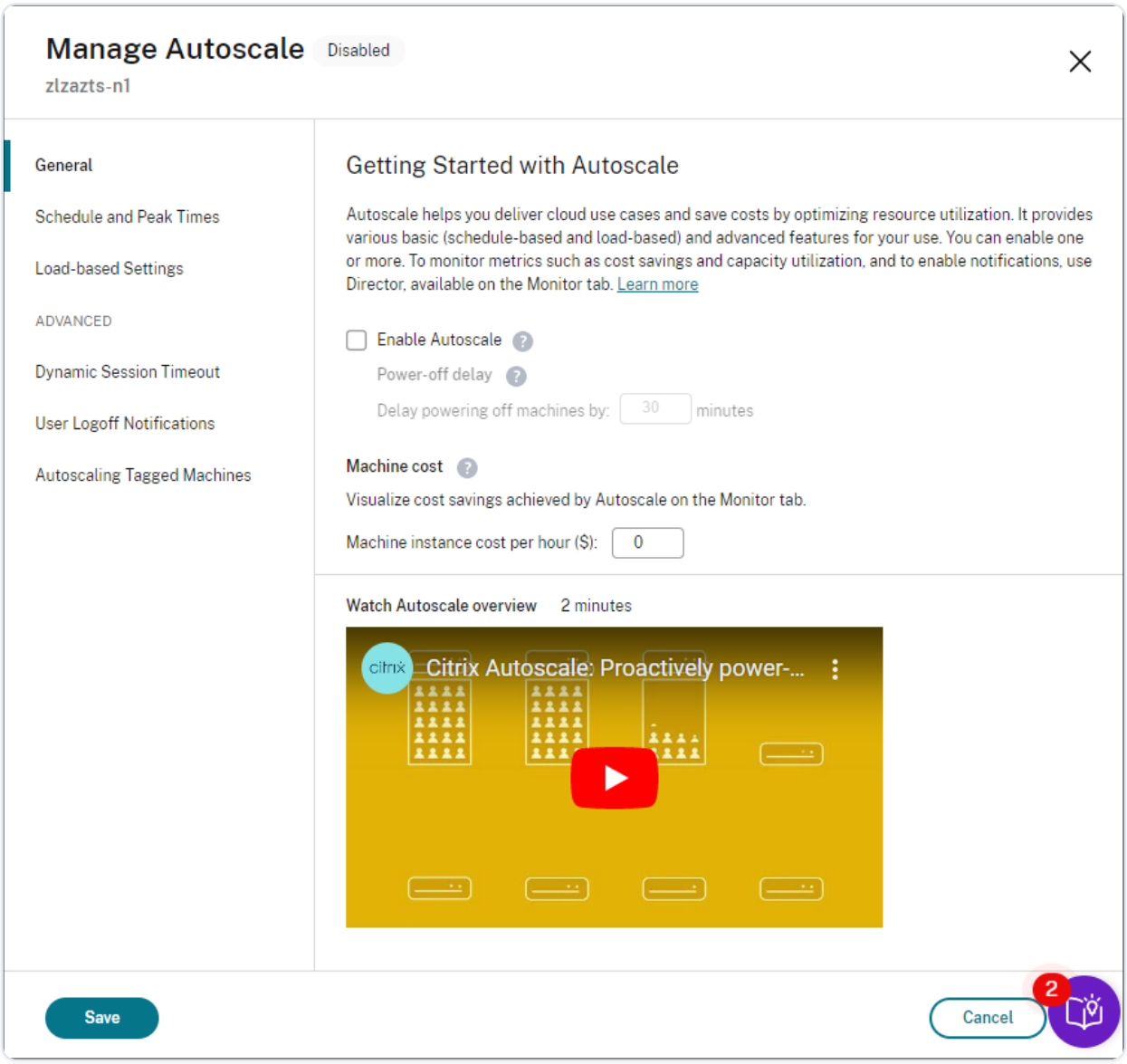
You can also use PowerShell commands to enable and configure Autoscale for a delivery group. For more information, see Broker PowerShell SDK commands.

1. From Studio, select **Delivery Groups** in the left pane.
2. Select the delivery group that you want to manage and then click **Manage Autoscale**.



3. On the **Manage Autoscale** page, select the **Enable Autoscale** checkbox to enable Autoscale. After you enable Autoscale, the options on the page are enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. To change the default settings based on your organization's needs, complete the following settings:

   - Set up schedules
   - To power off inactive machines more efficiently, use Dynamic session timeouts and User logoff notifications
   - To power manage a subset of machines in the delivery group, use Autoscaling tagged machines

To disable Autoscale, clear the **Autoscale** checkbox. The options on the page turn gray to indicate that Autoscale is disabled for the selected delivery group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

- If you disable Autoscale, all machines managed by Autoscale remain in their states at the time of disabling.
- After you disable Autoscale, the machines in drain state are taken out of drain state. For more information about drain state, see Drain state.
- The **Power policies** actions for single-session OS static delivery groups and single-session OS random delivery groups on the **Load-based Settings** page is independent of the Autoscale setting (enabled or disabled).

You can dynamically provision machines for the group using a PowerShell script. For more information, see Dynamic machine provisioning.

Autoscale options for VMs with user sessions

Autoscale can manage both assigned and pooled machines, optimizing their power and availability. The following content provides PowerShell commands and UI settings for controlling machine power states based on peak and off-peak times and user sessions for assigned and pooled machines.

Assigned machines are dedicated to a single user, while pooled machines are shared among multiple users.

NOTE:

- Session limit policies in Citrix Studio, particularly the *Disconnected session timer* and *Session idle timer*, are crucial for managing user sessions even when Citrix Autoscale is NOT enabled. These policies define how long a session can remain disconnected or idle before being terminated, ensuring resource utilization and preventing locked-out sessions. The policy setting can be used for both assigned and pooled machines, particularly those running multi-session VDAs. For detailed information, see Session limits policy settings.
- The `Get-BrokerMachine` PowerShell command is deprecated. Use `Get-BrokerMachineV2` as an alternative.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For assigned machines

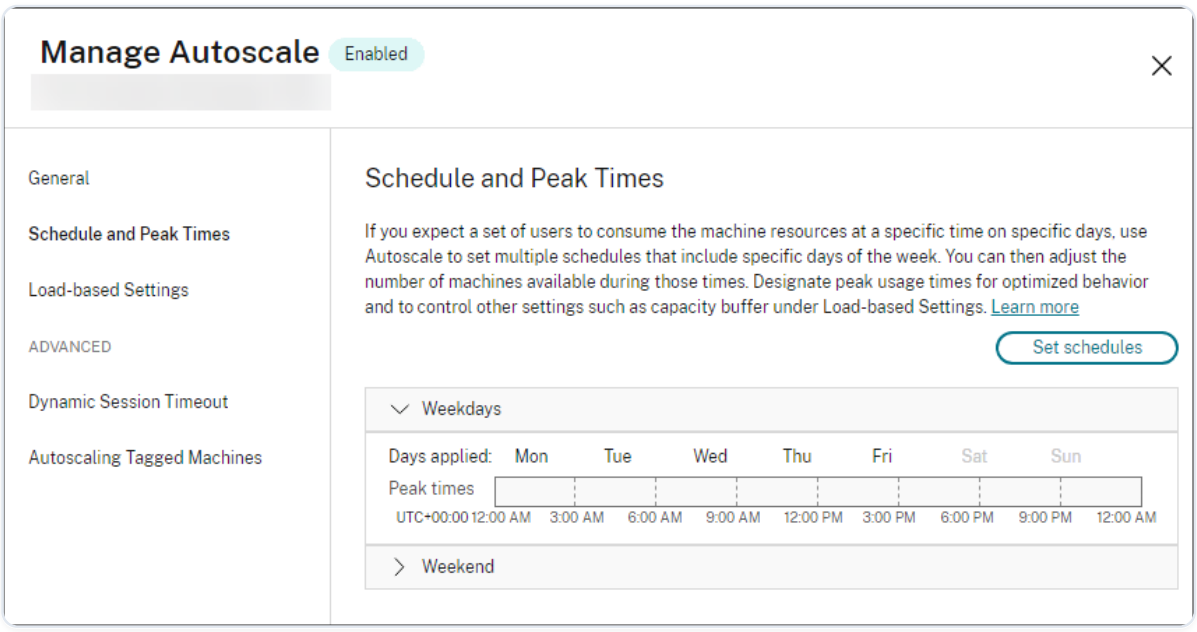
- To automatically power on assigned single-session machines in a static delivery group at the beginning of peak time use the PowerShell command:

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
```

- To ensure any assigned machine that is found to be off during peak time is restarted, also enable `AutomaticPowerOnForAssignedDuringPeak`.

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
-AutomaticPowerOnForAssignedDuringPeak $True
```

- If you want the VMs to turn on only when a user launches a session, then do either of the following:
  - Set `AutomaticPowerOnForAssigned` and `AutomaticPowerOnForAssignedDuringPeak` to `False`.
  - Define all hours as off-peak with no peak hours at all using the UI interface. See Schedule-based settings. During off peak times an Autoscale managed assigned machine is shut down if it has no user session on it.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In cases where all the machines are turned on by Autoscale at peak times, use the UI interface to set the wait time in minutes and actions like, no action, suspend, or shut down if no user logs on after the machine is powered on by Autoscale. See Power policies.

For pooled machines

To automatically shut down pooled machines after session logoff, set the PowerShell command `ShutdownAfterUse` to `True` for a delivery group. For example:

```
Set-BrokerDesktopGroup -Name “DesktopGroupName” -ShutdownDesktopsAfterUse
$true
```

Monitor metrics

After you enable Autoscale for a delivery group, you can monitor the following metrics of Autoscale-managed machines from the **Monitor** console.

- Machine usage
- Estimated savings
- Alert notifications for machines and sessions
- Machine status
- Load evaluation trends

NOTE:

When you initially enable Autoscale for a delivery group, it might take a few minutes to display monitoring data for that delivery group. Monitoring data remains available if Autoscale is enabled and then disabled for the delivery group. Autoscale collects monitoring data at 5-minute intervals.

For more information about the metrics, see Monitor Autoscale-managed machines.

Autoscale on hibernated VMs

You can hibernate VMs through configurable Autoscale settings. Use the PowerShell commands `Get-BrokerDesktopGroups`, `New-BrokerDesktopGroups`, or `Set-BrokerDesktopGroups` to set the following positive value to the parameter `AutoscaleScaleDownActionDuringPeak` (during peak) or `AutoscaleScaleDownActionDuringOffPeak` (during off peak) to define the power actions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 0: Shut down the VMs when scaling down
- 1: Suspend (hibernate the VMs) when scaling down

VMs not capable of hibernation are shut down.

You can configure reboot schedules for hibernated VMs if the Delivery Group is hibernation enabled. In the reboot cycle, the VMs are resumed and then shut down. The reboot schedule can be set as weekly, daily, monthly, and once. You can configure multiple schedules. However, the VMs resuming from hibernation can take a few mins.

Autoscale can also power on hibernated multi-session Remote Desktop Services (RDS) and shared single-session VMs with no sessions on it during peak time. The VMs can be of MCS and non-MCS machine catalogs.

More information

For more information on Autoscale, see Citrix Autoscale in Tech Zone.

Schedule-based and load-based settings

How Autoscale™ power manages machines

Autoscale powers machines on and off based on the selected schedule. Autoscale lets you set multiple schedules that include specific days of the week and adjust the number of machines available during those times. If you expect a set of users to consume the machine resources at a specific time on specific days, Autoscale helps provide an optimized experience. Note that those machines will be powered on during the schedule, whether or not there are sessions running on them.

NOTE:

Autoscale supports any power-managed machine.

The schedule is based on the **time zone** of the delivery group. To change the time zone, you can change user settings in a delivery group. For more information, see Manage Delivery Groups.

Autoscale has two default schedules: *Weekdays* (Monday through Friday) and *Weekend* (Saturday and Sunday). By default, the **Weekdays** schedule keeps one machine powered on from 07:00 AM to 06:30 PM during peak times and none during off-peak times. The default capacity buffer is set to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10% during peak and off-peak times. By default, the **Weekend** schedule keeps no machines powered on.

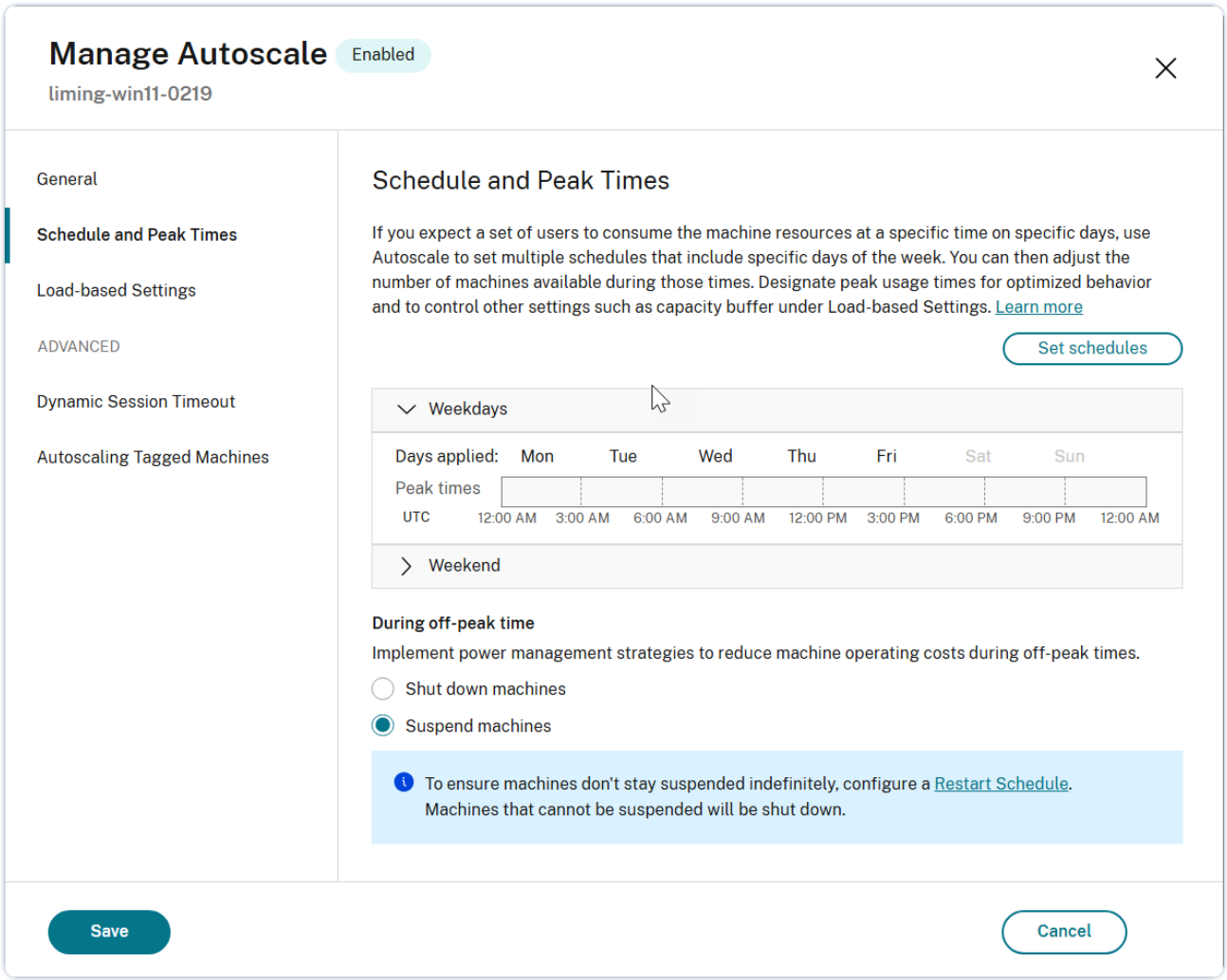
NOTE:

Autoscale treats only those machines that are registered with the site as part of the available capacity in the calculations it makes. "Registered" means that the machine is available for use or already in use. Doing so ensures that only machines that can accept user sessions are included in the capacity for the delivery group.

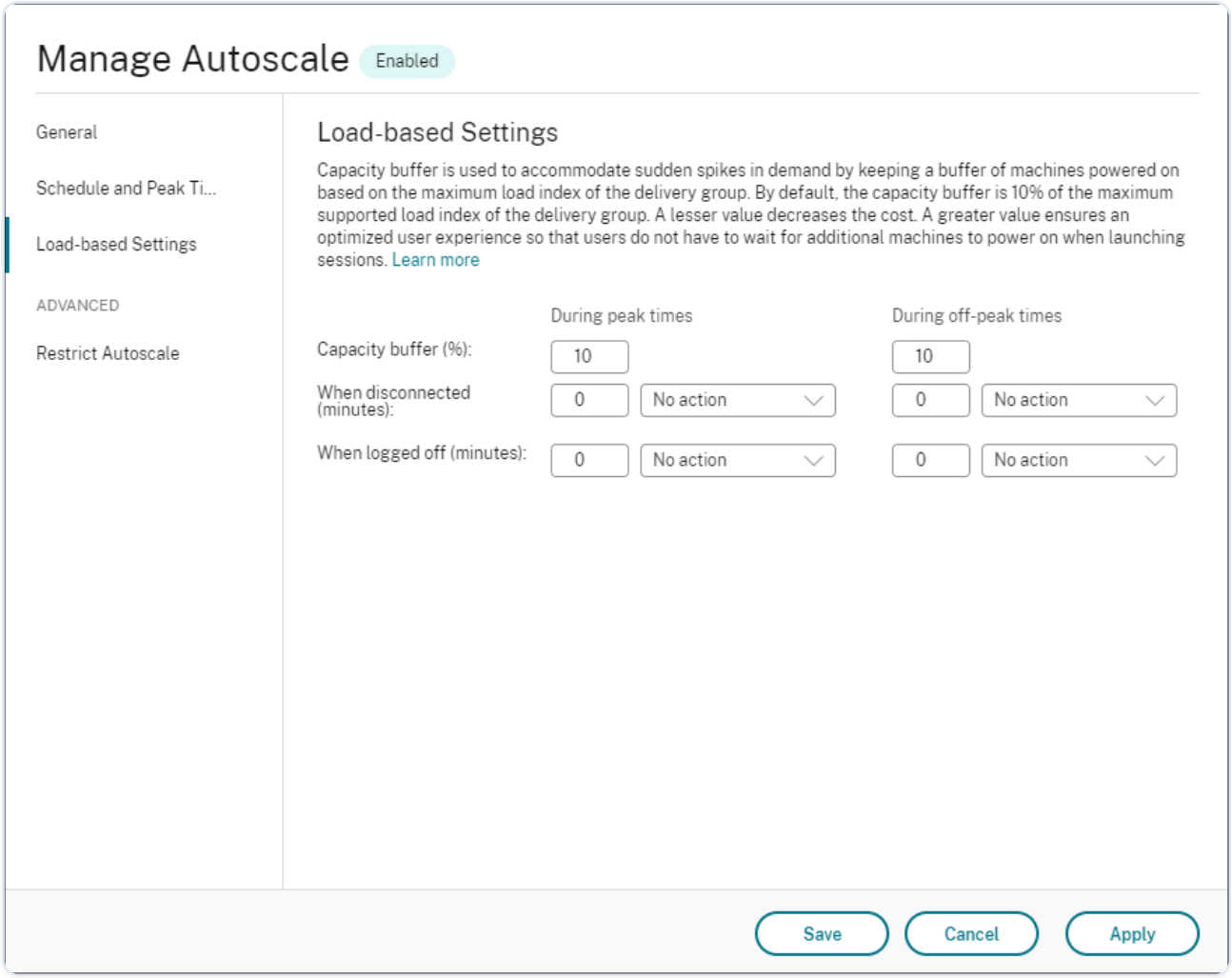
User interfaces

There are three types of user interfaces to be aware of.

User interface for *single-session OS static delivery groups*:

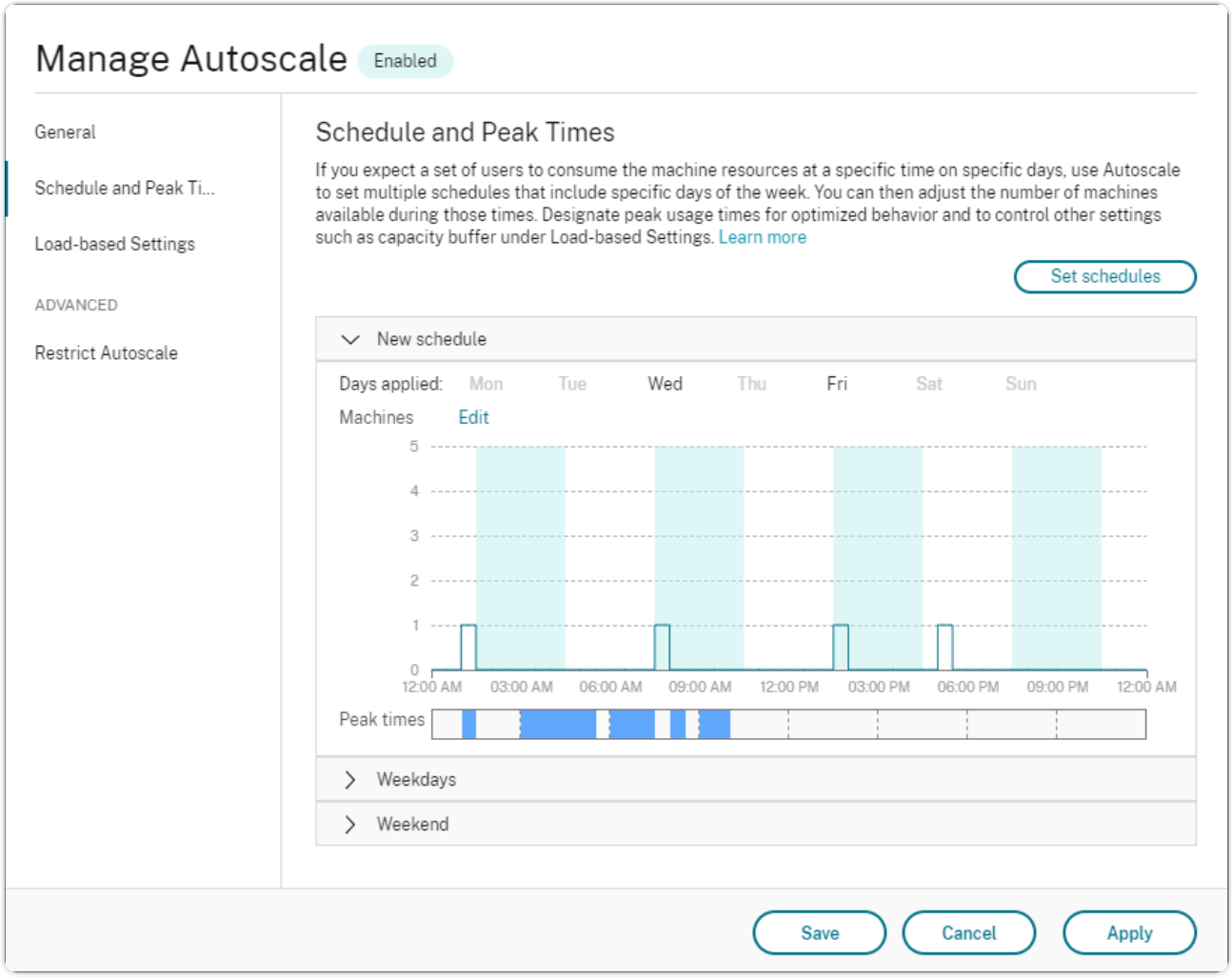


© 1997–2026 Citrix Systems, Inc. All rights reserved.

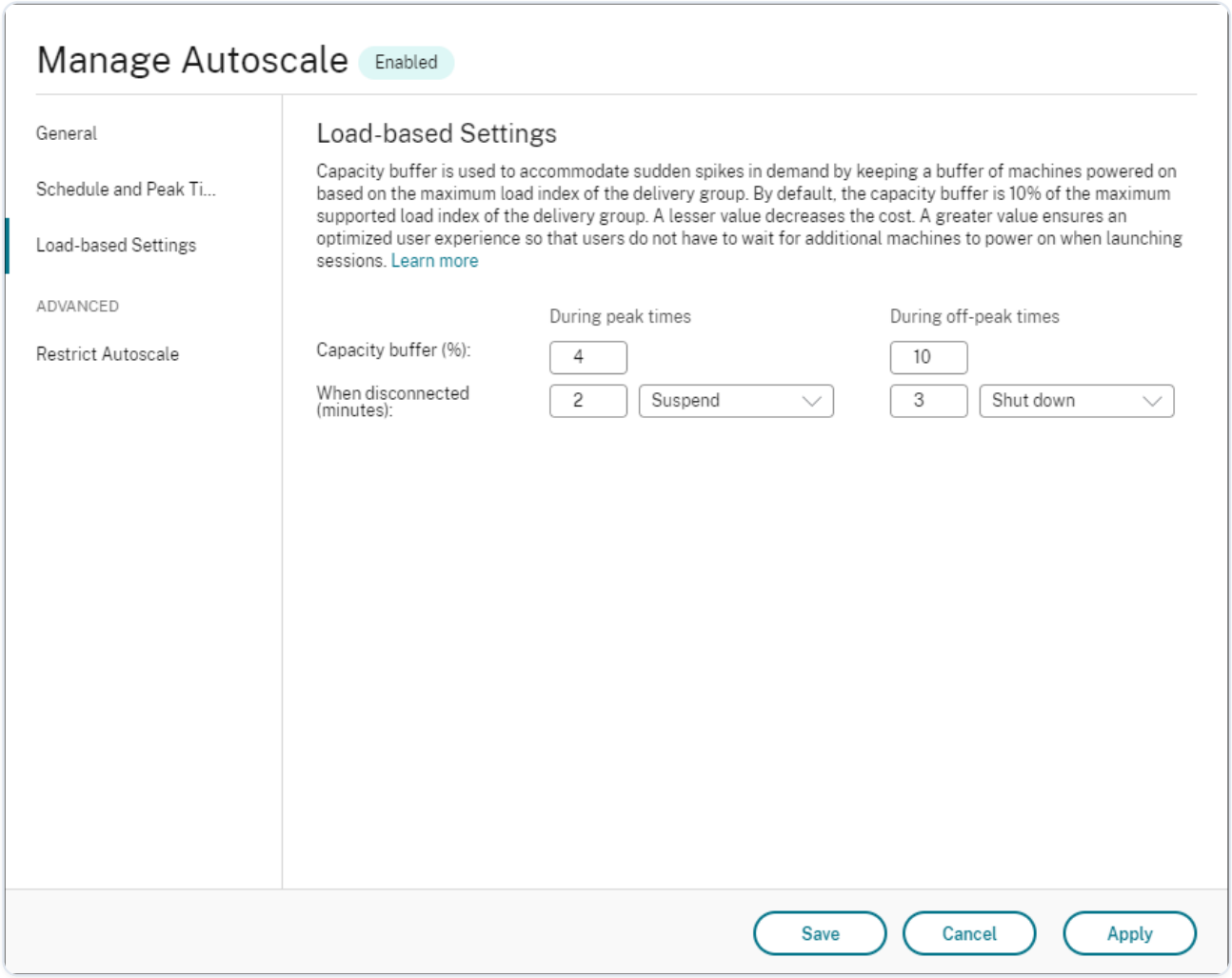


Autoscale user interface for *single-session OS random delivery groups*:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

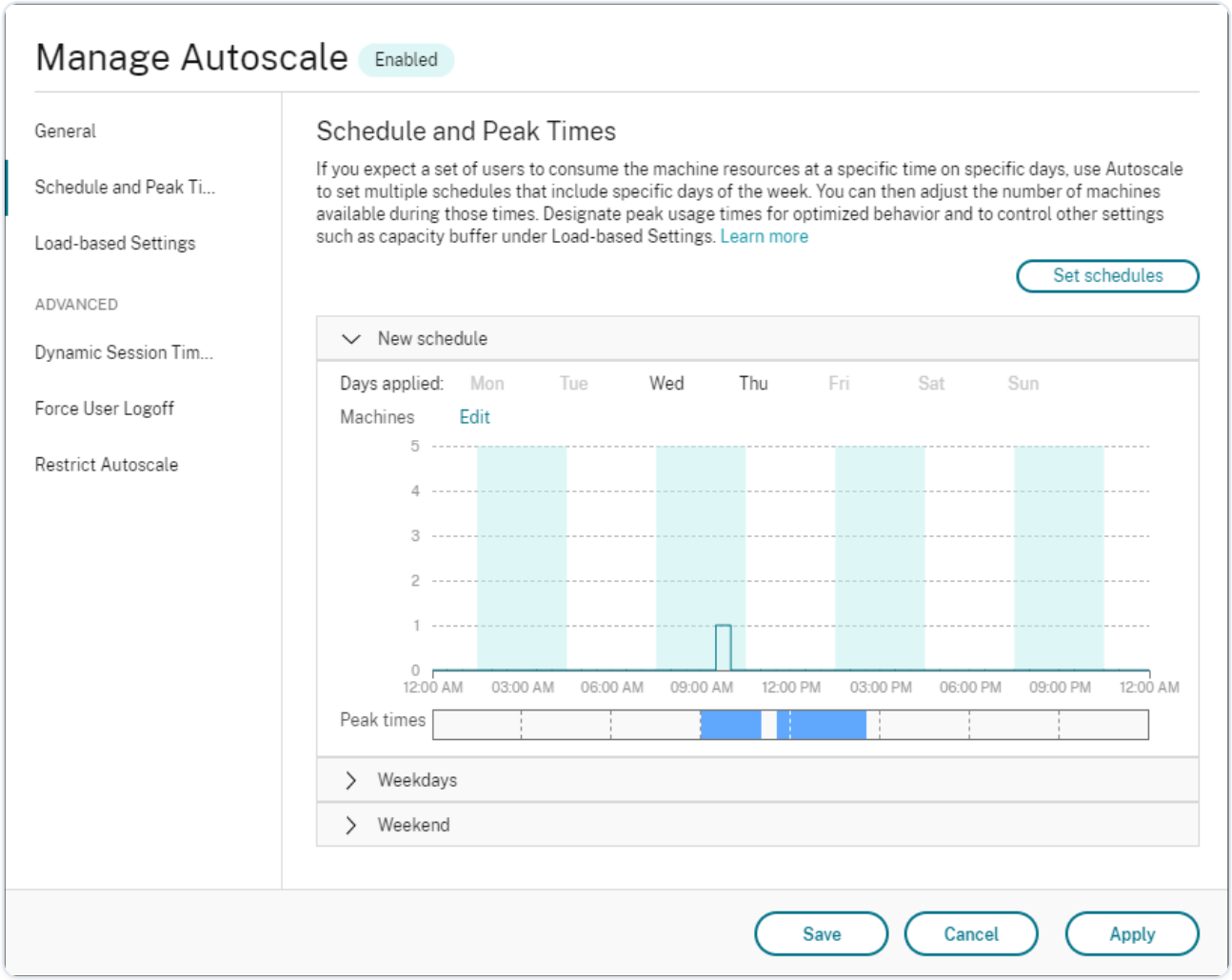


© 1997–2026 Citrix Systems, Inc. All rights reserved.

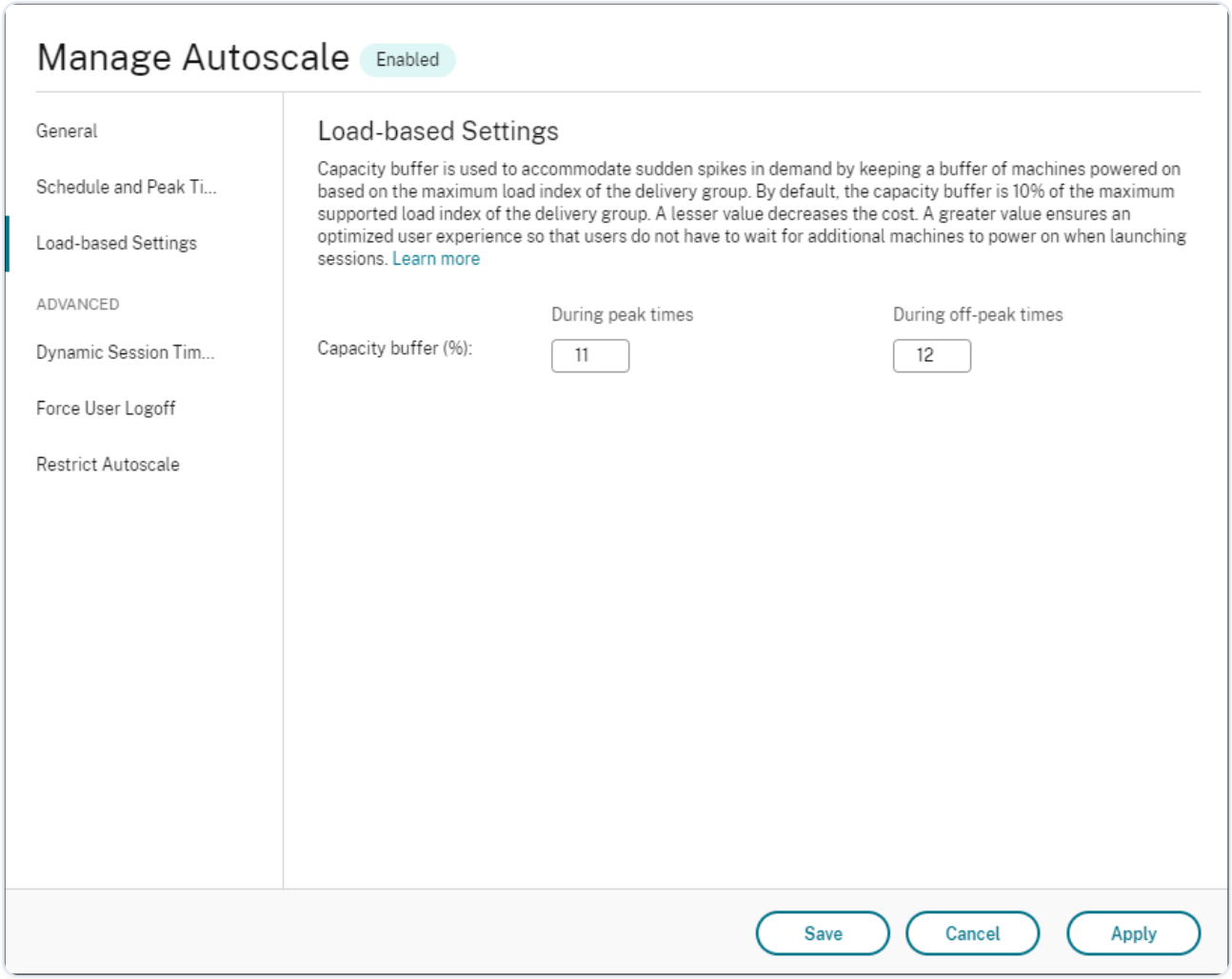


Autoscale user interface for *multi-session OS delivery groups*:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Schedule-based settings

Autoscale schedule. Lets you add, edit, select, and delete schedules.

Days applied. Highlights the days you applied to the selected schedule. The remaining days are grayed out.

Edit. Lets you assign the machines against each hour or each half hour. You can assign the machines by numbers and by percentages.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- This option is available only in the Autoscale user interfaces for multi-session OS and single-session OS random delivery groups.
- The histogram next to **Edit** plots the number or percentage of machines that are running in different time slots.
- You can **assign machines** against each time slot by clicking **Edit** above **Peak times**. Depending on the option you selected from the menu in the **Machines to start** window, you can assign the machines by numbers or by percentages.
- For multi-session OS delivery groups, you can set the minimum number of running machines separately in granular increments of 30 minutes during each day. For single-session OS random delivery groups, you can set the minimum number of running machines separately in granular increments of 60 minutes during each day.

To define your own schedules, follow these steps:

1. On the **Schedule and Peak Times** page of the **Manage Autoscale** window, click **Set schedules**.
2. In the **Edit Autoscale Schedules** window, select the days you want to apply to each schedule. You can also delete schedules as applicable.
3. Click **Done** to save the schedules and to return to the **Schedule and Peak Times** page.
4. Select the applicable schedule and configure it as needed.
5. Click **Apply** to exit the **Manage Autoscale** window or configure settings on other pages.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

- Autoscale does not allow the same day to overlap in different schedules. For example, if you select Monday in schedule2 after selecting Monday in schedule1, Monday is automatically cleared in schedule1.
- A schedule name is not case sensitive.
- A schedule name must not be blank or contain only spaces.
- Autoscale allows blank spaces between characters.
- A schedule name must not contain the following characters: \ / ; : # . * ? = < > \| ( ) { } " ' `.
- Autoscale does not support duplicate schedule names. Enter a different name for each schedule.
- Autoscale does not support empty schedules. This means that schedules without days selected are not saved.

Note:
The days included in the selected schedule are highlighted, while those not included are grayed out.

Restart schedule

Autoscale allows you to configure restart schedules to the suspended machines. This ensures that the systems remain efficient and avoid the systems being in suspended indefinitely.

To add a restart schedule for the suspended machines, do the following:

1. From Studio, select **Delivery Groups** in the left pane.
2. Right-click a delivery group that doesn't have a restart schedule and click **Manage Autoscale**.
    a. On the **General** page, select the **Enable Autoscale** check box.
    b. On the **Schedule and Peak Times** page, select the **Suspend machines** option during off-peak times. A tip to configure restart schedule is shown to avoid machines being in suspended state indefinitely.
    c. Click **Restart Schedule** in the tip information.
    d. Configure the preferred settings for **Restart frequency**, **Repeats every**, **Start date**, and **Begin restart at** and click **Done**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Load-based settings

Peak times. Lets you define the peak times for the days you applied in the selected schedule. You can do so by right-clicking the horizontal bar graph. After you define the peak times, the remaining, undefined times default to off-peak times. By **default**, the 7:00 AM to 7:00 PM time slot is defined as peak times for the days included in the selected schedule.

IMPORTANT:

- For multi-session OS delivery groups, the peak times bar graph is used for the capacity buffer.
- For single-session OS delivery groups, the peak times bar graph is used for the capacity buffer and controls the actions to be triggered after logoff and/or disconnection.
- You can define the peak times for the days included in a schedule at a granular level of 30 minutes for both multi-session OS and single-session OS delivery groups. Alternatively, you can use the `New-BrokerPowerTimeScheme PowerShell` command instead. For more information, see Broker PowerShell SDK commands.

Capacity buffer. Lets you keep a buffer of powered-on machines. A lesser value decreases the cost. A greater value ensures an optimized user experience so that when launching sessions, users do not have to wait for additional machines to power on. By default, the capacity buffer is 10% for peak and off-peak times. If you set the capacity buffer to 0 (zero), users might have to wait for additional machines to power on when launching sessions. Autoscale lets you determine the capacity buffer separately for peak and off-peak times.

Exclude machines in drain state from capacity buffer. When selected, machines that are currently draining (for example, due to a scheduled restart) are excluded from the capacity buffer calculation. Only machines that are fully available to accept new sessions are counted when determining required capacity. This helps prevent over-provisioning that can occur when draining machines are included in the buffer. By default, this option is not selected. This option is available only for multi-session OS delivery groups and requires Delivery Controller version 2503 or later.

Restart schedule

Autoscale allows you to configure restart schedules to the suspended machines. This ensures that the systems remain efficient and avoid the systems being in suspended indefinitely.

To add a restart schedule for the suspended machines, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. On the **Load-based Settings** page, under **Power policies > After disconnection**, select the suspend action. A tip to configure restart schedule is shown to avoid machines being in suspended state indefinitely.
2. Click **Restart Schedule** in the tip information.
3. Configure the preferred settings for **Restart frequency**, **Repeats every**, **Start date**, and **Begin restart at** and click **Done**.

Miscellaneous settings

TIP:

- You can choose to configure the miscellaneous settings using the Broker PowerShell SDK. For more information, see Broker PowerShell SDK commands.
- To understand the SDK commands associated with the when disconnected and when logged off settings, see `<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`.

When disconnected. Lets you specify how long a disconnected, locked machine remains powered on after session disconnection before it is suspended or shut down. If a time value is specified, the machine is suspended or shut down when the specified disconnection time elapses, depending on the action you configured. By default, no action is assigned to disconnected machines. You can define actions separately for peak and off-peak times. To do so, click the down arrow and then select one of the following options from the menu:

- **No action**. If selected, the machine after session disconnection remains powered on. Autoscale does not act on it.
- **Suspend**. If selected, Autoscale pauses the machine without shutting it down when the specified disconnection time elapses. The following option becomes available after you select **Suspend**.
    - **When no reconnection in (minutes)**. Suspended machines remain available to disconnected users when they reconnect but are not available for new users. To make the machines available again to handle all workloads, shut them down. Specify the timeout, in minutes, after which Autoscale shuts them down.
- **Shut down**. If selected, Autoscale shuts down the machine when the specified disconnection time elapses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

This option is available only in the Autoscale user interfaces for single-session OS random and static delivery groups.

When logged off. Lets you specify how long a machine remains powered on after session logoff before it is suspended or shut down. If a time value is specified, the machine is suspended or shut down when the specified logoff time elapses, depending on the actions you configured. By default, no action is assigned to logged-off machines. You can define actions separately for peak and off-peak times. To do so, click the down arrow and then select one of the following options from the menu:

- **No action**. If selected, the machine after session logoff remains powered on. Autoscale does not act on it.
- **Suspend**. If selected, Autoscale pauses the machine without shutting it down when the specified logoff time elapses.
- **Shut down**. If selected, Autoscale shuts down the machine when the specified logoff time elapses.

NOTE:

This option is available only in the Autoscale user interface for single-session OS static delivery groups.

Power manage single-session OS machines transitioning to a different time period with disconnected sessions

IMPORTANT:

- This enhancement applies only to single-session OS machines with disconnected sessions. It does not apply to single-session OS machines with logged off sessions.
- For this enhancement to take effect, you need to enable Autoscale for the applicable delivery group. Otherwise, disconnect power policy actions are not triggered on period transition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In earlier releases, a single-session OS machine transitioning to a time period where an action (disconnect action="**Suspend**" or "**Shutdown**") was required remained powered on. This scenario occurred if the machine disconnected during a time period (peak or off-peak times) where no action (disconnect action="**Nothing**") was required.

Starting with this release, Autoscale suspends or powers off the machine when the specified disconnection time elapses, depending on the disconnect action configured for the destination time period.

For example, you configure the following power policies for a single-session OS delivery group:

- Set `PeakDisconnectAction` to "Nothing"
- Set `OffPeakDisconnectAction` to "Shutdown"
- Set 'OffPeakDisconnectTimeout' to "10"

NOTE:

For more information about the disconnect action power policy, see `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` and `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`.

In earlier releases, a single-session OS machine with a session disconnected during peak times remained powered on when it transitioned from peak to off-peak. Starting with this release, the `OffPeakDisconnectAction` and the `OffPeakDisconnectTimeout` policy actions are applied to the single-session OS machine on period transition. As a result, the machine is powered off 10 minutes after it transitions to off-peak.

In case you want to revert to the previous behavior (that is, take no action on machines that transition from peak to off-peak or off-peak to peak with disconnected sessions), do one of the following:

- Set the "LegacyPeakTransitionDisconnectedBehaviour" registry value to 1 (true; enables the previous behavior). By default, the value is 0 (false; triggers disconnect power policy actions on period transition).
  - Path: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Name: LegacyPeakTransitionDisconnectedBehaviour

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - Type: REG_DWORD
  - Data: 0x00000001 (1)

- Configure the setting by using the `Set-BrokerServiceConfigurationData` PowerShell command. For example:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

A machine must meet the following criteria before power policy actions can be applied to it on period transition:

- Has a disconnected session.
- Has no pending power actions.
- Belongs to a single-session OS delivery group that transitions to a different time period.
- Has a session that disconnects during a certain time period (peak or off-peak times) and transitions to a period where a power action is assigned.

How capacity buffer works

Capacity buffer is used to add spare capacity to the current demand to account for dynamic load increases. There are two scenarios to be aware of:

- For multi-session OS delivery groups, the capacity buffer is defined as a percentage of the total capacity of the delivery group in terms of load index. For more information about load index, see Load index.
- For single-session OS delivery groups, the capacity buffer is defined as a percentage of the total capacity of the delivery group in terms of the number of machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- In scenarios where you restrict Autoscale to tagged machines, the capacity buffer is defined as a percentage of the total capacity of the tagged machines in the delivery group in terms of load index.
- For multi-session OS delivery groups, when the **Exclude machines in drain state from capacity buffer** option is enabled, draining machines are excluded from the total capacity calculation. Autoscale powers on additional machines as needed to maintain the configured buffer percentage, based only on machines that are fully available to accept new sessions.

Autoscale lets you set the capacity buffer separately for peak and off-peak times. A lesser value in the capacity buffer field decreases the cost because Autoscale powers on less spare capacity. A greater value ensures an optimized user experience so that users do not have to wait for additional machines to power on when launching sessions. By default, the capacity buffer is 10%.

IMPORTANT:

The capacity buffer results in machines being powered on when the total spare capacity drops to a level below "X" percent of the total capacity of the delivery group. Doing so reserves the required percentage of spare capacity.

Multi-session OS delivery groups

When are machines powered on?

IMPORTANT:

If a schedule is selected, Autoscale powers on all machines configured to be powered on in the schedule. Autoscale keeps this specified number of machines powered on during the schedule, regardless of the load.

When the number of powered-on machines in the delivery group can no longer meet the buffer needed for honoring the buffer capacity in terms of load index, Autoscale powers on extra machines. For example, let's say your delivery group has 20 machines and 3 machines are scheduled to be powered on as part of schedule-based scaling with a capacity buffer of 20%.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Eventually, 4 machines will be powered on when there is no load. This is because a 4 x 10k load index is needed as a buffer; therefore at least 4 machines need to be powered on. This case might occur during peak times, increased load on machines, new session launches, and when you add new machines to the delivery group. Note that Autoscale powers on only the machines that meet the following criteria:

- The machines are not in maintenance mode.
- The hypervisor on which the machines are running is not in maintenance mode.
- The machines are currently powered off.
- The machines have no pending power actions.

EXCLUDE DRAINING MACHINES FROM CAPACITY BUFFER

By default, draining machines (for example, those restarting on schedule) count toward total capacity when Autoscale calculates the buffer. You can exclude them so that the buffer is based only on machines that are fully available to accept new sessions.

To exclude machines in drain state from the capacity buffer:

1. In **Web Studio**, select **Delivery Groups** in the left pane.
2. Right-click a multi-session OS delivery group and select **Manage Autoscale**.
3. On the **Load-based Settings** page, under **Capacity buffer**, select **Exclude machines in drain state from capacity buffer**.
4. Click **Save**.

NOTE:

This option is available only for multi-session OS delivery groups and requires Delivery Controller version 2503 or later.

When are machines powered off?

IMPORTANT:

- If a schedule is selected, Autoscale powers off the machines based on the schedule.
- Autoscale does not power off the machines configured in the schedule to be powered on during the schedule.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When there are more than enough machines to support the targeted number of powered-on machines (including the buffer) for the delivery group, Autoscale powers off extra machines. This case might occur during off-peak times, decreased load on machines, and session logoffs, and when you remove machines from the delivery group. Autoscale powers off only the machines that meet the following criteria:

- The machines and the hypervisor on which the machines are running are not in maintenance mode.
- The machines are currently powered on.
- The machines are registered as available or waiting to register after start-up.
- The machines have no active sessions.
- The machines have no pending power actions.
- The machines satisfy the specified power-off delay. This means that the machines have been powered on for at least "X" minutes, where "X" is the power-off delay specified for the delivery group.

Example scenario

Suppose you have the following scenario:

- **Delivery group configuration**. The delivery group that you want Autoscale to power manage contains 10 machines (M1 to M10).
- **Autoscale configuration**
  - Capacity buffer is set to 10%.
  - No machine is included in the selected schedule.

The scenario is executed in the following sequence:

1. No user logs on.
2. User sessions increase.
3. More user sessions start.
4. User session load decreases because of session termination.
5. User session load decreases further until the session load is handled only by on-premises resources.

See below for details about how Autoscale works in the scenario above.

- No user load (initial state)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - One machine (for example, M1) is powered on. The machine is powered on because of the configured capacity buffer. In this case, 10 (number of machines) x 10,000 (load index) x 10% (configured capacity buffer) equals 10,000. Therefore, one machine is powered on.
    - The load index value of the powered-on machine (M1) is at a baseline load (load index equals 0).

- The first user logs on
    - The session is directed to be hosted on machine M1.
    - The load index of the powered-on machine M1 increases and machine M1 is no longer at a baseline load.
    - Autoscale starts to power on an additional machine (M2) to meet the demand because of the configured capacity buffer.
    - The load index value of machine M2 is at a baseline load.
- Users increase load
    - The sessions are load-balanced across machines M1 and M2. As a result, the load index of the powered-on machines (M1 and M2) increases.
    - The total spare capacity is still at a level above 10,000 in terms of load index.
    - The load index value of machine M2 is no longer at a baseline load.
- More user sessions start
    - The sessions are load-balanced across machines (M1 and M2). As a result, the load index of the powered-on machines (M1 and M2) increases further.
    - When the total spare capacity drops to a level below 10,000 in terms of load index, Autoscale starts to power on an additional machine (M3) to meet the demand because of the configured capacity buffer.
    - The load index value of machine M3 is at a baseline load.
- Even more user sessions start
    - The sessions are load-balanced across machines (M1 to M3). As a result, the load index of the powered-on machines (M1 to M3) increases.
    - The total spare capacity is at a level above 10,000 in terms of load index.
    - The load index value of machine M3 is no longer at a baseline load.
- User session load decreases because of session termination

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - After users log off from their sessions or idle sessions time out, the freed-up capacity on machines M1 to M3 is reused to host sessions started by other users.
    - When the total spare capacity increases to a level above 10,000 in terms of load index, Autoscale puts one of the machines (for example, M3) into drain state. As a result, sessions started by other users are no longer directed to that machine unless new changes occur. For example, end-user load increases again or other machines become least loaded.

- User session load continues to decrease
    - After all sessions on machine M3 are terminated and the specified power-off delay times out, Autoscale powers off machine M3.
    - After more users terminate their sessions, the freed-up capacity on powered-on machines (M1 and M2) is reused to host sessions started by other users.
    - When the total spare capacity increases to a level above 10,000 in terms of load index, Autoscale puts one of the machines (for example, M2) into drain state. As a result, sessions started by other users are no longer directed to that machine.
- User session load continues to decrease until there are no sessions
    - After all sessions on machine M2 are terminated and the specified power-off delay times out, Autoscale powers off machine M2.
    - The load index value of the powered-on machine (M1) is at a baseline load. Autoscale does not put machine M1 into drain state because of the configured capacity buffer.

NOTE:

For multi-session OS delivery groups, all changes to the desktop are lost when users log off sessions. However, if configured, user-specific settings are roamed along with the user profile.

Single-session OS random delivery groups

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the total number of machines in the delivery group. By default, the capacity buffer is 10% of the total number of machines in the delivery group.

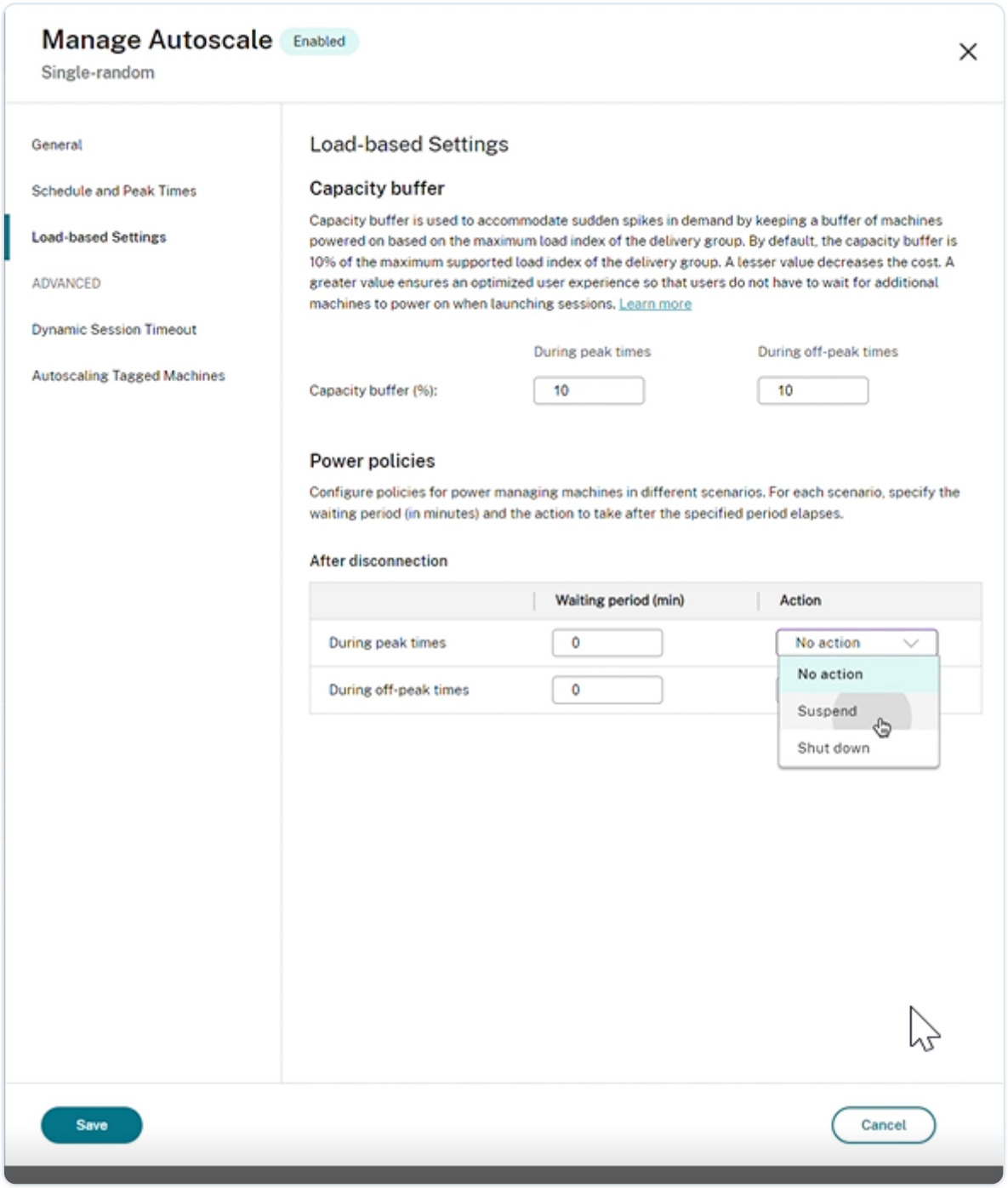
If the number of machines (including the capacity buffer) exceeds the total number of currently powered-on machines, additional machines are powered on to meet the demand. If the number of machines (including the capacity buffer) is less than the total number of currently powered-on

© 1997–2026 Citrix Systems, Inc. All rights reserved.

machines, the excess machines are shut down or suspended, depending on the actions you configured.

Power policies

Configure policies to manage the power of the machines for different scenarios. For each scenario, you can specify the wait time (in minutes) and the action to take after the specified time ends. Power policies are applicable for Single-session OS random delivery groups and Single-session OS static delivery groups.



After disconnection, the following settings are applicable for both during peak times and during off-peak times:

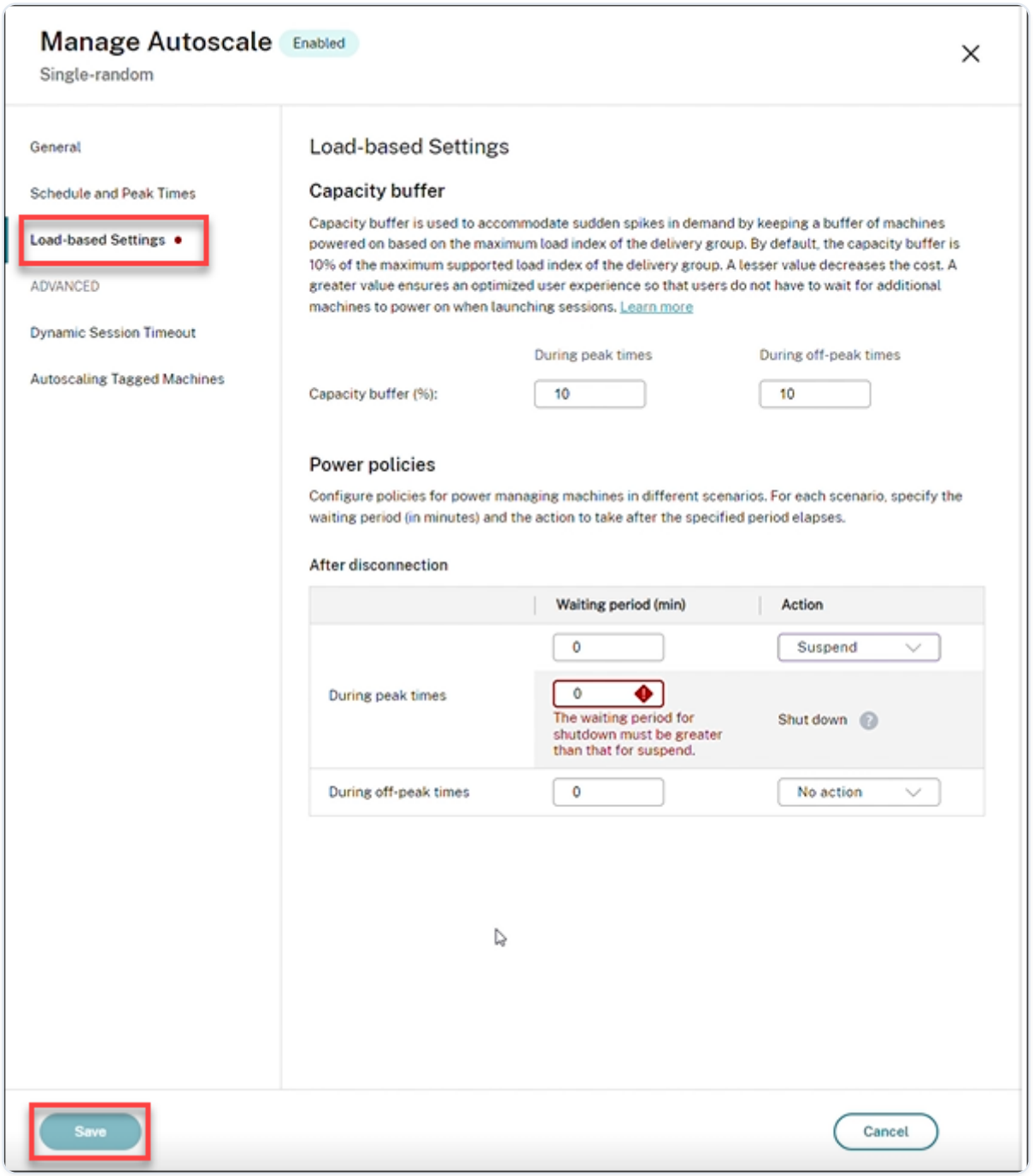
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can set the wait time in minutes and actions like, no action, suspend, or shut down from the drop down.
- If you select the suspend action, configure an additional wait time to shut down the machine.

NOTE:

- During peak and off-peak times, the wait time for shutdown action must be greater than the wait time of suspend.
- Suspended machines are accessible only to disconnected users when they reconnect. To make the suspended machines available for new users, shut them down.
- If the time settings are incorrectly configured for suspend and shut down fields, the **Save** option is disabled and a red dot also appears next to the navigation items indicating setting errors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For example

- If you set the wait time to 12 minutes and choose the first action to be no action, then after the end of 12 minutes, the machine will continue to be in powered on state.
- If you set the wait time to 15 minutes and choose the first action to be suspend and the second wait time to be 20 minutes, after the end of 15 minutes, the machine will be suspended. After the end of the second wait time, the machine will be shut down.
- If you set the wait time to 18 minutes and choose the first action to be shut down, then after the end of 18 minutes, the machine will be shut down.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example scenario

Suppose you have the following scenario:

- **Delivery group configuration**. The delivery group that you want Autoscale to power manage contains 10 machines (M1 to M10).
- **Autoscale configuration**
  - Capacity buffer is set to 10%.
  - No machine is included in the selected schedule.

The scenario is executed in the following sequence:

1. No user logs on.
2. User sessions increase.
3. More user sessions start.
4. User session load decreases because of session termination.
5. User session load decreases further until the session load is handled only by on-premises resources.

See below for details about how Autoscale works in the scenario above.

- No user load (initial state)
  - One machine (M1) is powered on. The machine is powered on because of the configured capacity buffer. In this case, 10 (number of machines) x 10% (configured capacity buffer) equals 1. Therefore, one machine is powered on.
- A first user logs on
  - The first time a user logs on to use a desktop, the user is assigned a desktop from a pool of desktops hosted on powered-on machines. In this case, the user is assigned a desktop from machine M1.
  - Autoscale starts to power on an additional machine (M2) to meet the demand because of the configured capacity buffer.
- A second user logs on
  - The user is assigned a desktop from machine M2.
  - Autoscale starts to power on an additional machine (M3) to meet the demand because of the configured capacity buffer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A third user logs on
  - The user is assigned a desktop from machine M3.
  - Autoscale starts to power on an additional machine (M4) to meet the demand because of the configured capacity buffer.
- A user logs off
  - After a user logs off or the user's desktop times out, the freed-up capacity (for example, M3) is available as buffer. As a result, Autoscale starts to power off machine M4 because the capacity buffer is configured as 10%.
- More users log off until there are no users
  - After more users log off, Autoscale powers off machines (for example, M2 or M3).
  - Even though there are no users left, Autoscale does not power off the remaining one machine (for example, M1) because that machine is reserved as a spare capacity.

NOTE:

For single-session OS random delivery groups, all changes to the desktop are lost when users log off sessions. However, if configured, user-specific settings are roamed along with the user profile.

Single-session OS static delivery groups

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of unassigned machines powered on based on the total number of unassigned machines in the delivery group. By default, the capacity buffer is 10% of the total number of unassigned machines in the delivery group.

IMPORTANT:

After all machines in the delivery group are assigned, the capacity buffer does not play a role in powering machines on or off.

If the number of machines (including the capacity buffer) exceeds the total number of currently powered-on machines, additional, unassigned machines are powered on to meet the demand. If the number of machines (including the capacity buffer) is less than the total number of currently

© 1997–2026 Citrix Systems, Inc. All rights reserved.

powered-on machines, excess machines are powered off or suspended, depending on the actions you configured.

For single-session OS static delivery groups, Autoscale:

- Powers assigned machines on during peak times and off during off-peak times only when the `AutomaticPowerOnForAssigned` property of the applicable single-session OS delivery group is set to true.
- Automatically powers on a machine during peak times if it is powered off and the `AutomaticPowerOnForAssignedDuringPeak` property of the delivery group to which it belongs is set to true.

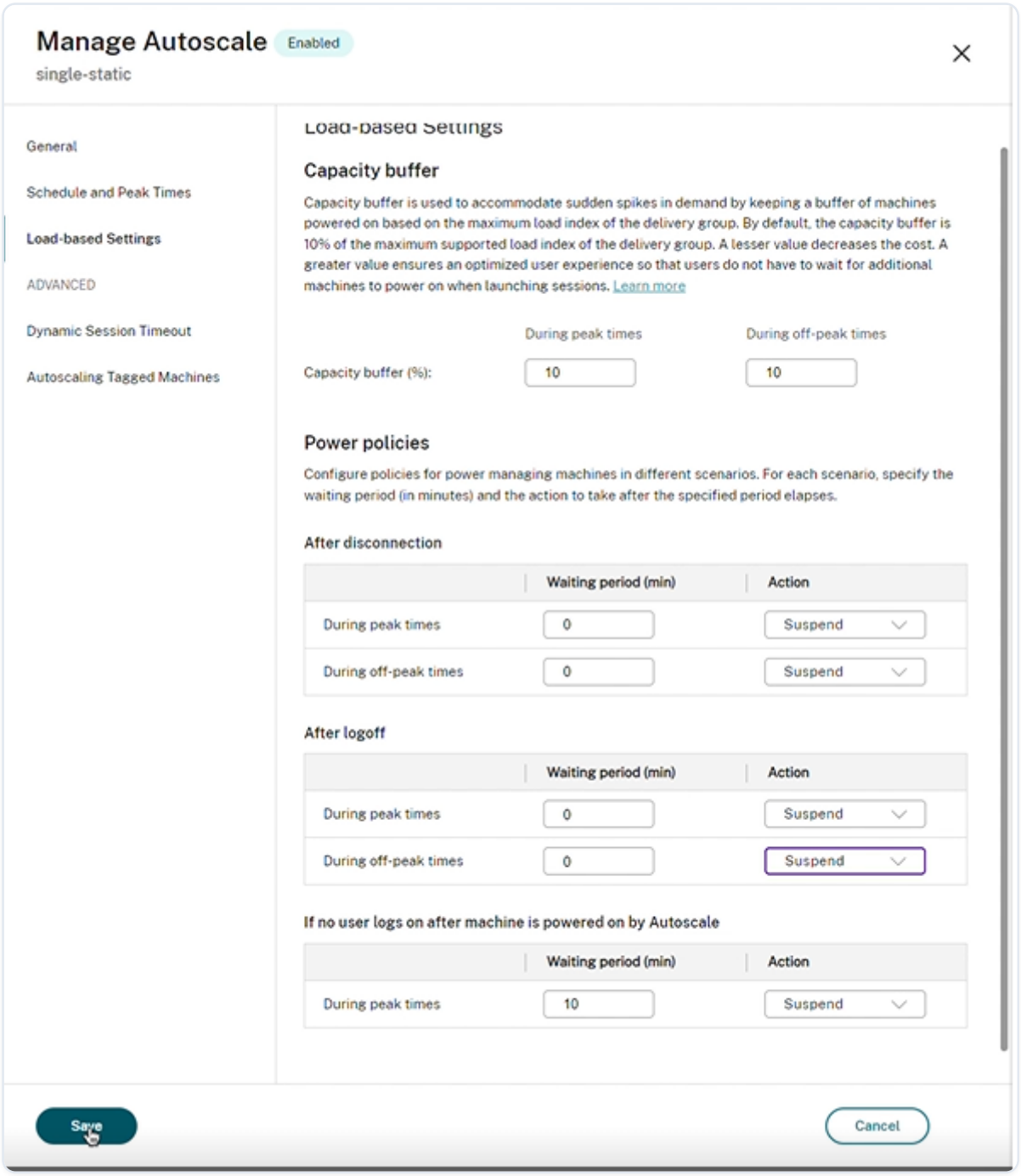
To understand how capacity buffer works with assigned machines, consider the following:

- The capacity buffer works only when the delivery group has one or more unassigned machines.
- If the delivery group has no unassigned machines (all machines in the delivery group are assigned), the capacity buffer does not play a role in powering machines on or off.
- The `AutomaticPowerOnForAssignedDuringPeak` property determines whether assigned machines are powered on during peak times. If it is set to true, Autoscale keeps the machines powered on during peak times. Autoscale will also power them on even if they are powered off.

Power policies

Configure policies to manage the power of the machines for different scenarios. For each scenario, you can specify the wait time (in minutes) and the action to take after the specified time ends. Power policies is applicable for Single-session OS random delivery groups and Single-session OS static delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For **After disconnection** and **After logoff**, the following settings are applicable for both, during peak times and during off-peak times: You can set the wait time in minutes and actions like, no action, suspend, or shut down from the drop down.

If no user logs on after machine is powered on by Autoscale, the following settings are applicable only during peak times: You can set the wait time in minutes and actions like, no action, suspend, or shut down from the drop down during peak times.

Example scenario

Suppose you have the following scenario:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Delivery group configuration**. The delivery group that you want Autoscale to power manage contains 10 machines (M1 to M10).
- **Autoscale configuration**
  - Machines M1 to M3 are assigned, and machines M4 to M10 are unassigned.
  - Capacity buffer set to 10% for peak and off-peak times.
  - According to the selected schedule, Autoscale power manages machines between 09:00 AM and 06:00 PM.

See below for details about how Autoscale works in the scenario above.

- Start of schedule – 09:00 AM
  - Autoscale powers on machines M1 to M3.
  - Autoscale powers on an additional machine (for example, M4) because of the configured capacity buffer. Machine M4 is unassigned.
- A first user logs on
  - The first time a user logs on to use a desktop, the user is assigned a desktop from a pool of desktops hosted on unassigned powered-on machines. In this case, the user is assigned a desktop from machine M4. Subsequent logons from that user connect to the same desktop that was assigned on first use.
  - Autoscale starts to power on an additional machine (for example, M5) to meet the demand because of the configured capacity buffer.
- A second user logs on
  - The user is assigned a desktop from the unassigned powered-on machines. In this case, the user is assigned a desktop from machine M5. Subsequent logons from that user connect to the same desktop that was assigned on first use.
  - Autoscale starts to power on an additional machine (for example, M6) to meet the demand because of the configured capacity buffer.
- Users log off
  - As users log off from their desktops or the desktops time out, Autoscale keeps the machines M1 to M5 powered on during 09:00 AM – 06:00 PM. When those users log on the next time, they connect to the same desktop that was assigned on first use.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - The unassigned machine M6 is waiting to serve a desktop to an incoming, unassigned user.

- End of schedule – 06:00 PM
    - At 06:00 PM, Autoscale powers off machines M1 to M5.
    - Autoscale keeps the unassigned machine M6 powered on because of the configured capacity buffer. That machine is waiting to serve a desktop to an incoming, unassigned user.
    - In the delivery group, machines M6 to M10 are unassigned machines.

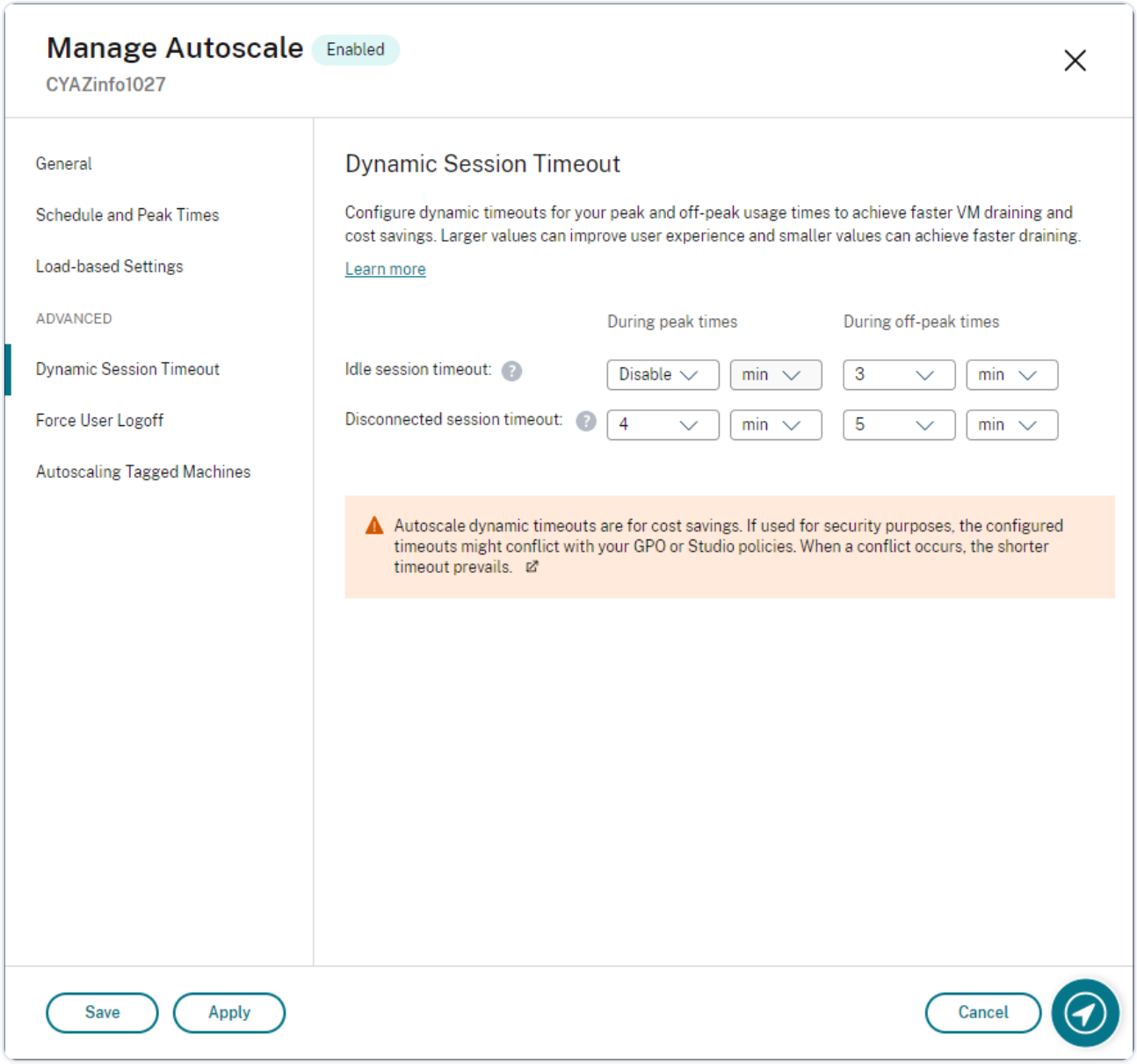
Dynamic session timeouts

This feature lets you configure disconnected and idle session timeouts for your peak and off-peak usage times to achieve faster machine draining and cost savings. This feature applies to:

- Single-session and multi-session OS machines.
- All machines in the Delivery Group regardless of whether they are tagged for autoscaling.

A VDA reports idle times for sessions that have been idle for more than 10 minutes, so dynamic session timeouts will not be able to disconnect idle sessions within 10 minutes of being idle. A lesser value removes lingering sessions sooner, thus reducing costs.

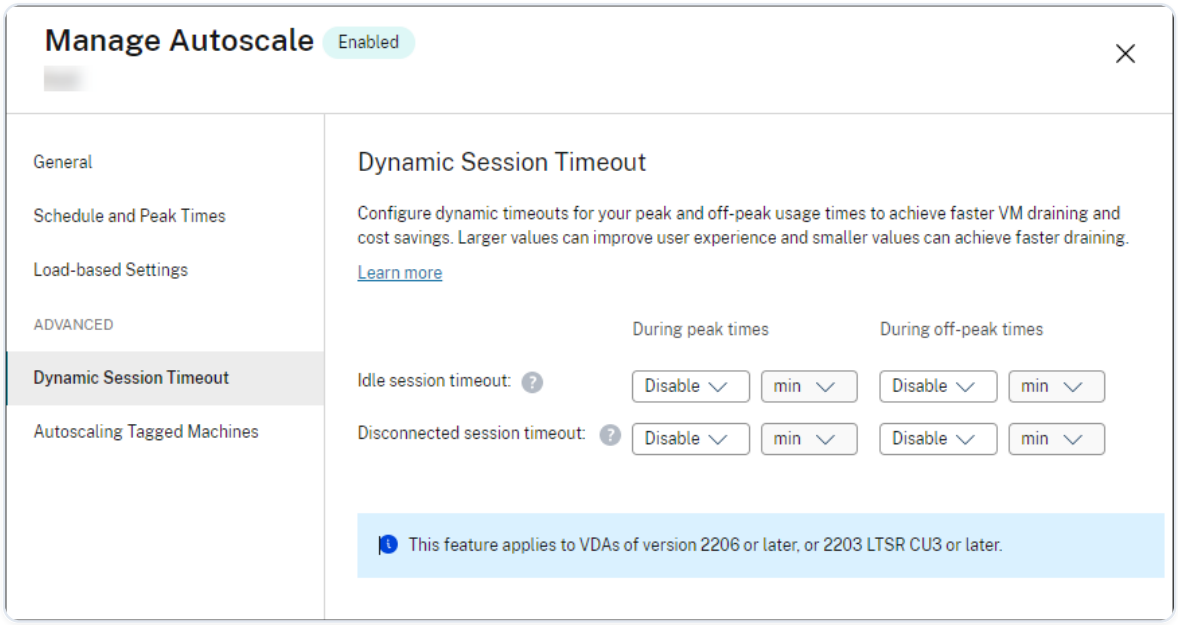
© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- This feature is always available for multi-session OS delivery groups.
- For single-session OS delivery groups, this feature applies to VDAs of version 2206 CR or later, or 2203 LTSR CU3 or later. Ensure that those VDAs have registered with Citrix Cloud™ at least once. When unavailable, the following user interface appears:



- Autoscale™ dynamic timeouts are for cost savings. If used for security purposes, the configured timeouts might conflict with your GPO or Studio policies. When a conflict occurs, the shorter timeout prevails.

Idle session timeout. Enables or disables a timer that specifies how long an uninterrupted user connection is maintained if there is no user input. When the timer expires, the session is placed in the disconnected state and the **Disconnected session timeout** applies. If the **Disconnected session timeout** is disabled, the session is not logged off.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

- If you specify a value less than or equal to 10 minutes (600 seconds), Autoscale disconnects the relevant sessions after they have been idle for 10 minutes. This is because Autoscale relies on session idle times that VDAs report. VDAs report idle times only for sessions that have been idle for more than 10 minutes.
- An idle session will still be placed into a disconnected state if the user interacts with it within the last 5 minutes of reaching the idle session timeout.

Disconnected session timeout. Enables or disables a timer that specifies how long a disconnected desktop remains locked before the session is logged off. If enabled, the disconnected session is logged off when the timer expires.

FAQ

Does the dynamic session timeout feature apply only to machines tagged for Autoscaling?

The dynamic session timeout feature applies to all the machines in the Delivery group, regardless of whether they are tagged for autoscaling.

When a session is logged off due to dynamic session timeout, are untagged machines also included in the Autoscale target of tagged machines?

The dynamic session timeout feature is not related to the Autoscale tagging feature. If dynamic session timeouts result in sessions being terminated, untagged machines might also be shut down during the process provided the machines are draining until shut down.

Autoscaling tagged machines (cloud burst)

NOTE:

This feature was formerly Restrict Autoscale.

Introduction

Autoscale provides the flexibility to power manage only a subset of machines in a delivery group. To achieve this, apply a tag to one or more machines and then configure Autoscale to power manage only tagged machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature can be useful in cloud bursting use cases, where you want to use on-premises resources (or reserved public cloud instances) to handle workloads before cloud-based resources address additional demand (that is, burst workloads). To let on-premises machines (or reserved instances) address workloads first, you must use tag restriction along with zone preference.

Tag restriction specifies machines to be power managed by Autoscale. Zone preference specifies machines in the preferred zone to handle user launch requests. For more information, see Tags and Zone preference.

To autoscale certain tagged machines, you can use Studio or PowerShell.

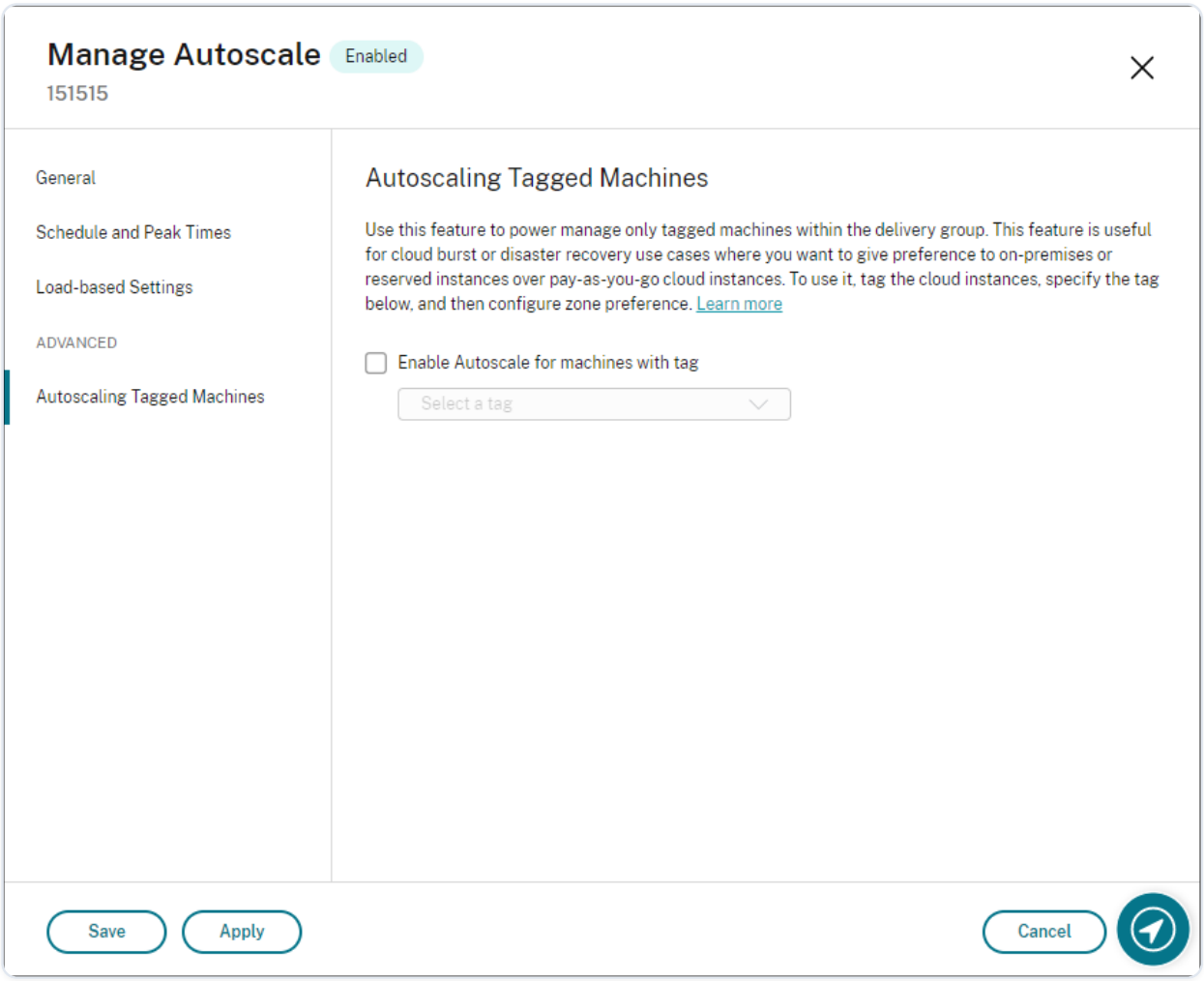
Use Studio to autoscale certain tagged machines

To autoscale certain tagged machines, complete the following steps:

1. Create a tag and apply that tag to the applicable machines in the delivery group. For more information, see Manage tags and tag restrictions.
2. Select the delivery group and then open the **Manage Autoscale** wizard.
3. On the **Autoscaling Tagged Machines** page, select **Enable Autoscale for machines with tag**, select a tag from the list, and then click **Apply** to save your changes.

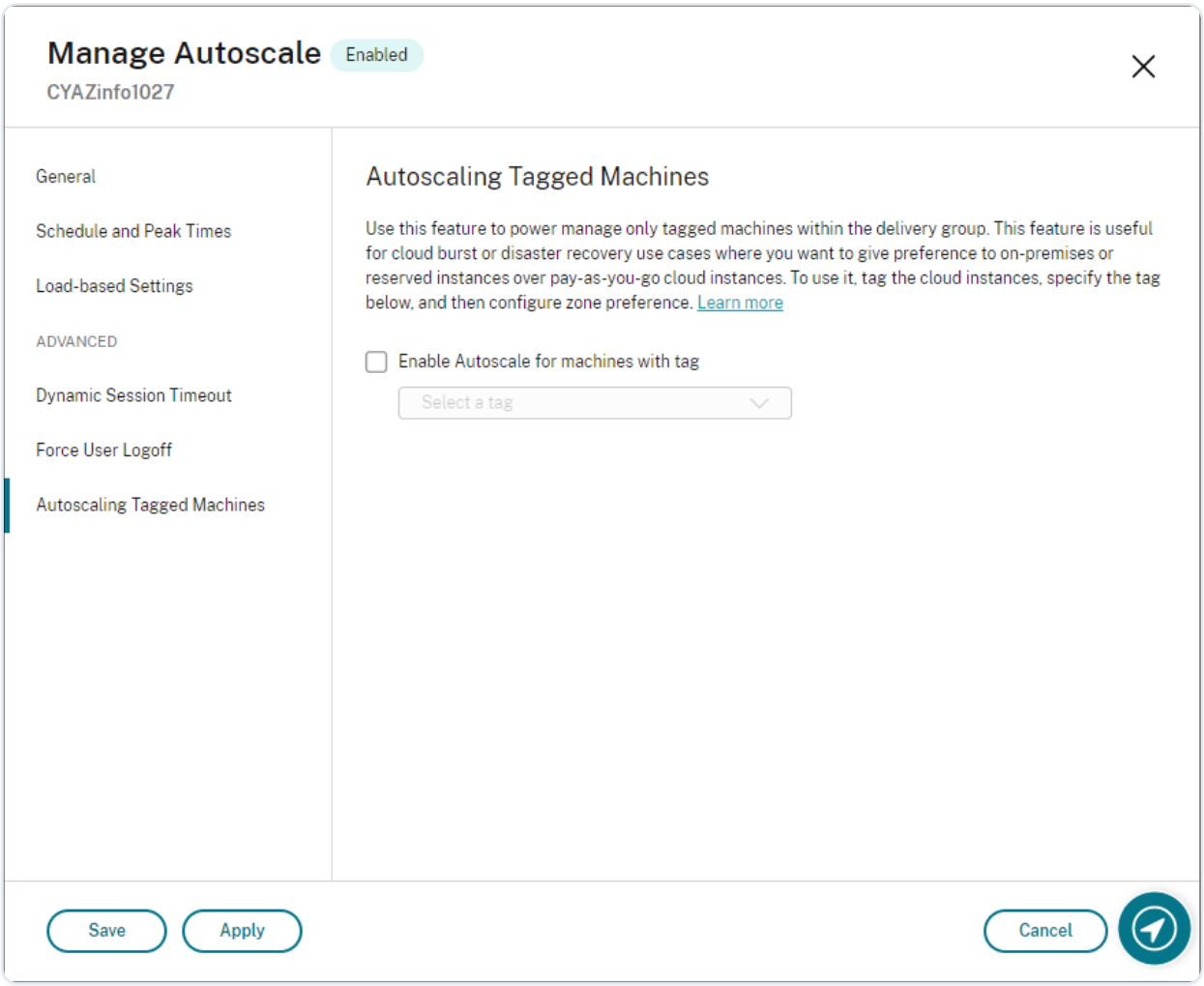
   User interface for single-session OS *static* and *random* delivery groups:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



User interface for *multi-session OS delivery groups*:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



WARNING:

- Autoscaling machines with a specific tag might cause the histogram to update automatically to reflect the number of machines per the tag. On the **Schedule and Peak Times** page, you can manually assign machines against each time slot if needed.
- You cannot delete a tag that is being used on tagged machines. To delete the tag, you must first remove the tag restriction.

After you apply the tag restriction, you might want to remove it from the delivery group later. To do so, go to the **Manage Autoscale > Autoscaling Tagged Machines** page and then clear **Enable Autoscale for machines with tag**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WARNING:

- If you remove the tag from the applicable machines without clearing **Enable Autoscale for machines with tag**, you might receive a warning when you open the **Manage Autoscale** wizard. Removing the tag from the machines can leave no machines for Autoscale to manage because the tag you specified in Autoscale has become invalid. To resolve the warning, go to the **Autoscaling Tagged Machines** page, remove the invalid tag, and then click **Apply** to save your changes.

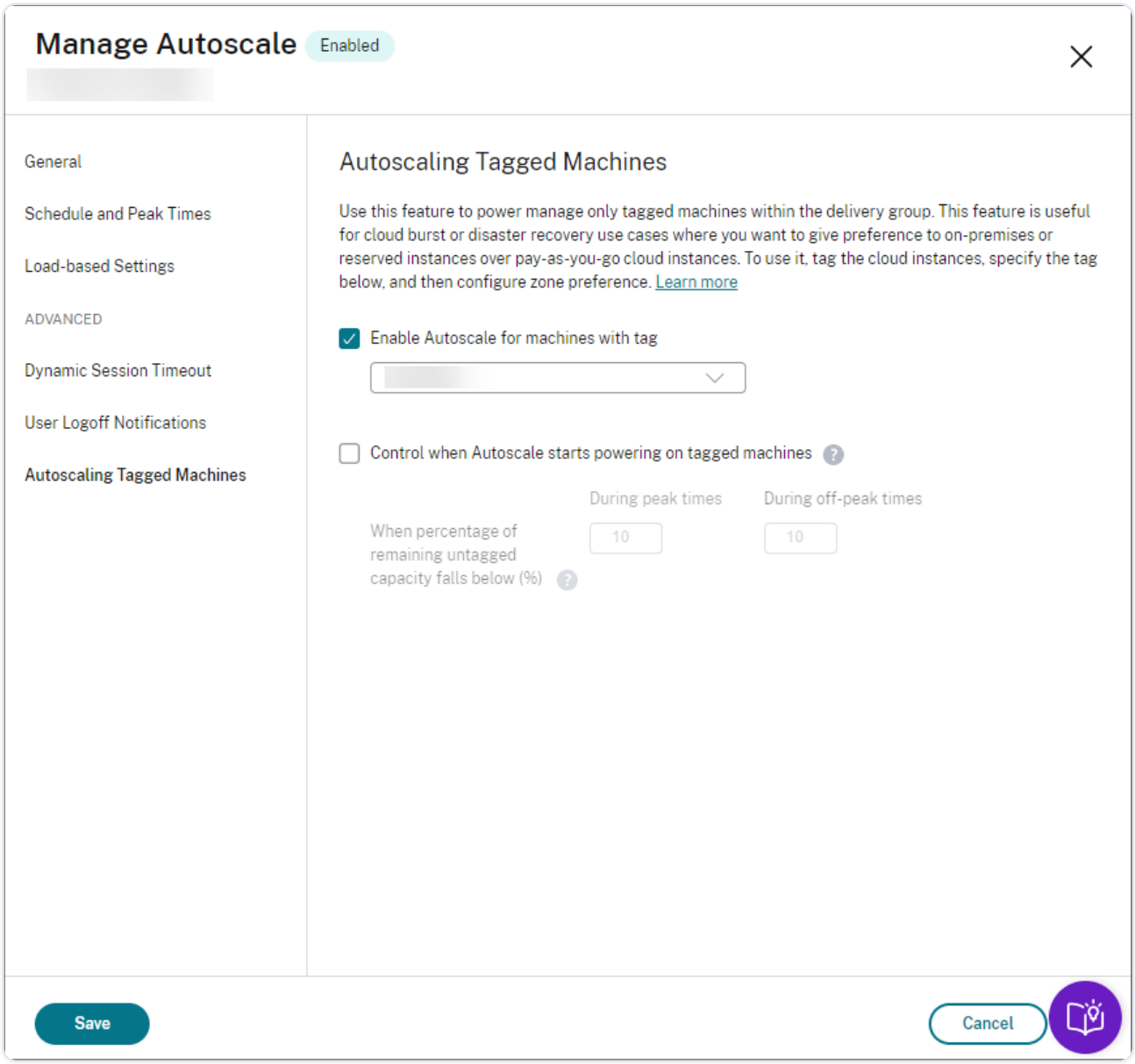
Control when Autoscale powers on resources

You can also control when Autoscale starts powering on tagged machines based on the usage of untagged machines. This helps you further optimize the consumption of your tagged or public cloud workloads.

To do this, complete the following steps:

1. On the **Autoscaling Tagged Machines** page, select **Control when Autoscale starts powering on tagged machines**.
2. Enter the percentage amount of untagged machine usage you want to reach for both peak times and off-peak times and then click **Apply**. Supported values: 0–100.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



TIP:

The percentage controls when Autoscale starts powering on tagged machines. When the percentage falls below the threshold (default, 10%), Autoscale starts powering on tagged machines. When the percentage exceeds the threshold, Autoscale goes into power-off mode. When entering the percentage, consider two scenarios:

- For single-session OS delivery groups: The value is defined as a percentage of the total number of untagged machines in idle state. Example: You have 10 untagged single-session OS machines. When only one is left without a session, Autoscale starts powering on a tagged machine.
- For multi-session OS delivery groups: The value is defined as a percentage of the total capacity (in terms of load index) of available untagged machines. Example: You have 10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

untagged multi-session OS machines. When they are 90% loaded, Autoscale starts powering on a tagged machine.

Use PowerShell to autoscale certain tagged machines

NOTE:

The `Get-BrokerMachine` PowerShell command is deprecated. Use `Get-BrokerMachineV2` as an alternative.

To use the PowerShell SDK directly, complete the following steps:

1. **Create a tag.** Use the New-Brokertag PowerShell command to create a tag.
   - For example: `$managed = New-BrokerTag Managed`. In this case, the tag is named "Managed." For more information about the New-Brokertag PowerShell command, see `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`.
2. **Apply the tag to machines**. Use the `Get-Brokermachine` PowerShell command to apply the tag to machines in a catalog that you want Autoscale to power manage.
   - For example: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. In this case, the catalog is named "cloud."
   - For more information about the Get-Brokermachine PowerShell command, see `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`.

   NOTE:

   You might add new machines to the catalog after applying the tag. The tag is *NOT* automatically applied to those new machines.
3. **Add tagged machines to the delivery group that you want Autoscale to power manage.** Use the Get-BrokerDesktopGroup PowerShell command to add a tag restriction to the delivery group that contains the machines (in other words, "restrict launches to machines with tag X").

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For example: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. In this case, the UID of the Delivery Group is 1.
- For more information about the Get-BrokerDesktopGroup PowerShell command, see `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`.

After you apply the tag restriction, you might want to remove it from the delivery group later. To do so, use the Get-BrokerDesktopGroup PowerShell command.

Example: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`. In this case, the UID of the delivery group is 1.

NOTE:

Untagged machines restart automatically after users power them off. This behavior ensures that they become available to handle workloads sooner. This can be enabled or disabled on a per desktop group using the `Set-BrokerDesktopGroup`'s `AutomaticRestartForUntaggedMachines` property. For more information, see `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`.

Example scenario

Suppose you have the following scenario:

- **Machine catalog configuration**. There are two machine catalogs (C1 and C2).
  - Catalog C1 contains 5 machines (M1 to M5) that are local in the on-premises deployments.
  - Catalog C2 contains 5 machines (M6 to M10) that are remote in the cloud deployments.
- **Tag restriction**. A tag named "Cloud" is created and applied to machines M6 to M10 in catalog C2.
- **Zone configuration**. Two zones (Z1 and Z2) are created.
  - Zone Z1 containing catalog C1 corresponds to the on-premises deployments.
  - Zone Z2 containing catalog C2 corresponds to the cloud deployments.
- **Delivery group configuration**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - The delivery group contains 10 machines (M1 to M10), 5 machines from catalogs C1 (M1 to M5) and 5 from catalog C2 (M6 to M10).
    - Machines M1 to M5 are powered on manually and remain powered on throughout the schedule.

- **Autoscale configuration**
    - Capacity buffer is set to 10%.
    - Autoscale power manages only machines with the tag "Cloud." In this case, Autoscale power manages cloud machines M6 to M10.

- **Published application or desktop configuration**. Zone preferences are configured for the published desktops (for example), where Zone Z1 is preferred over Zone Z2 for a user launch request.
    - Zone Z1 is configured as the preferred zone (home zone) for the published desktops.

The scenario is executed in the following sequence:

1. No user logs on.
2. User sessions increase.
3. User sessions increase further until all available on-premises machines are consumed.
4. More user sessions start.
5. User session decreases because of session termination.
6. User session decreases further until the session load is handled only by on-premises machines.

See below for details about how Autoscale works in the scenario above.

- No user load (initial state)
    - The on-premises machines M1 to M5 are all powered on.
    - One machine in the cloud (for example, M6) is powered on. The machine is powered on because of the configured capacity buffer. In this case, 10 (number of machines) x 10,000 (load index) x 10% (configured capacity buffer) equals 10,000. Therefore, one machine is powered on.
    - The load index value of all the powered-on machines (M1 to M6) is at a baseline load (load index equals 0).
- Users log on

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - The sessions are directed to be hosted on machines M1 to M5 through the configured zone preference and are load-balanced across these on-premises machines.
    - The load index value of the powered-on machines (M1 to M5) increases.
    - The load index value of the powered-on machine M6 is at a baseline load.

- Users increase load, consuming all on-premises resources
    - The sessions are directed to be hosted on machine M1 to M5 through the configured zone preference and are load-balanced across these on-premises machines.
    - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
    - The load index value of the powered-on machine M6 remains at a baseline load.

- One more user logs on
    - The session overflows the zone preference and is directed to be hosted on cloud machine M6.
    - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
    - The load index value of the powered-on machine M6 increases and is no longer at a baseline load. When the total spare capacity drops to a level below 10,000 in terms of load index, Autoscale starts to power on an additional machine (M7) to meet the demand because of the configured capacity buffer. Note that it might take some time to power on machine M7. So there might be a delay until machine M7 is ready.

- More users log on
    - The sessions are directed to be hosted on machine M6.
    - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
    - The load index value of the powered-on machine M6 increases further, but the total spare capacity is at a level above 10,000 in terms of load index.
    - The load index value of the powered-on machine M7 remains at a baseline load.

- Even more users log on
    - After machine M7 is ready, the sessions are directed to be hosted on machines M6 and M7 and are load-balanced across these machines.
    - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
    - The load index value of machine M7 is no longer at a baseline load.
    - The load index value of the powered-on machines (M6 and M7) increases.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - The total spare capacity is still at a level above 10,000 in terms of load index.

- User session load decreases because of session termination

    - After users log off from their sessions or idle sessions time out, the freed-up capacity on machines M1 to M7 is reused to host sessions started by other users.
    - When the total spare capacity increases to a level above 10,000 in terms of load index, Autoscale puts one of the cloud machines (M6 to M7) into drain state. As a result, sessions started by other users are no longer directed to that machine (for example, M7) unless new changes occur; for example, user load increases again or other cloud machines become least loaded.

- User session load decreases further until one or more cloud machines are no longer needed

    - After all sessions on machine M7 are terminated and the specified power-off delay times out, Autoscale powers off machine M7.
    - The load index value of all the powered-on machines (M1 to M5) might drop to a level below 10,000.
    - The load index value of the powered-on machine (M6) decreases.

- User session decreases further until no cloud machines are needed.

    - Even though there are no user sessions on machine M6, Autoscale does not power it off because it is reserved as a spare capacity.
    - Autoscale keeps the remaining cloud machine M6 powered on because of the configured capacity buffer. That machine is waiting to serve a desktop to an incoming user.
    - Sessions are not directed to be hosted on machine M6 as long as the on-premises machines have available capacity.

Dynamic machine provisioning

Autoscale™ provides the capability to create machines and delete them dynamically. You can leverage the capability by using a PowerShell script. The script helps you dynamically scale up or down the number of machines in the delivery group based on the current load conditions.

The script offers the following benefits (and more):

- **Reducing storage costs**. Different from Autoscale, which helps reduce your computing costs, the script provides a more cost-effective solution to provision machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Effectively handling load changes**. The script helps you handle load changes by automatically scaling up or down the number of machines based on the current delivery group load.

Download the script

The PowerShell script is available at `<https://github.com/citrix/Powershell-Scripts/tree/master/XAXD/AutoscaleMcs>`.

How the script works

IMPORTANT:

- You cannot specify a machine catalog in more than one delivery group that is to be managed by the script. In other words, if multiple delivery groups share the same machine catalog, the script does not work with any of those delivery groups.
- You cannot concurrently run the script for the same delivery group from multiple locations.

The script works at a delivery group level. It measures the load (in terms of load index) and then determines whether to create or delete machines.

Machines created through this script are uniquely tagged (through the `ScriptTag` parameter) so that they can be identified later. Creating or deleting machines is based on:

- **Maximum percentage load of a delivery group**. Specifies the maximum level at which to create machines for Autoscale to address extra loads. When this threshold is exceeded, machines are created in batches to ensure that the current load decreases to or below the threshold.
- **Minimum percentage load of a delivery group**. Specifies the minimum level at which to delete machines created through this script that have no active sessions. When this threshold is exceeded, machines created through this script that have no active sessions are deleted.

This script is intended to monitor across a delivery group and to create or delete machines when the trigger criterion is met. It executes on a per-run basis. This means that you need to run the script on a regular basis so that it can function as intended. We recommend that you run the script at a minimum interval of five minutes. Doing so improves overall responsiveness.

The script relies on the following parameters to work:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	TYPE	DEFAULT VALUE	DESCRIPTION
DeliveryGroupName	String	X	Name of the delivery group to be monitored to determine the current load. You can provide a semicolon-separated list of names. For example: `Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile`.
XdProfileName	String	X	Name of the profile to use for authenticating to remote servers. For details about authenticating to remote servers using this parameter, see Authentication API.
HighWatermark	Integer	80	Maximum percentage load (in terms of load index) at which to create machines for Autoscale to address extra loads.
LowWatermark	Integer	15	Minimum percentage load (in terms of load index) at which to delete machines created through this

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	TYPE	DEFAULT VALUE	DESCRIPTION
			script that have no active sessions.
MachineCatalogName	String	X	Name of the machine catalog where machines are to be created.
MaximumCreatedMachines	Integer	-1	Maximum amount of machines that can be created in a specified delivery group. If the value is equal to or less than 0, the script does not process this parameter.
ScriptTag	String	AutoscaledScripted	Tag that applies to machines created through the script.
EventLogSource	String	X	Source name that appears in Windows Event Viewer.

NOTE:

An "X" indicates that no default value is specified for that parameter.

By default, the script requires all parameters (except the `ScriptTag` parameter) the first time it runs. On subsequent runs, only the `DeliveryGroupName` and the `XdProfileName` parameters are required. Optionally, you can choose to update the minimum and maximum percentage loads.

Note that you must specify a single delivery group the first time you run the script. For example, the script does *not* work if you use the following PowerShell command to specify two delivery groups the first time you run the script:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Instead, first specify a single delivery group (in this example, dg1) using the following command:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1' -XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Then, use the following command to run the script for the second delivery group (in this example, dg 2):

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile`

Prerequisites

To run the script, make sure that these prerequisites are met:

- The machine resides within the same domain where machines are being created.
- Remote PowerShell SDK is installed on that machine. For more information about the Remote PowerShell SDK, see SDKs and APIs.
- Other prerequisites:
  - A delivery group to monitor
  - A machine catalog created through Machine Creation Services™ (MCS) that has an associated provisioning scheme (template)
  - An identity pool that is associated with the provisioning scheme
  - An event log source to be created so that the script can write information to the Windows Event Log
  - A secure client that allows you to authenticate to remote servers

Permissions, recommendations, and notices

When you run the script, keep the following in mind:

- To authenticate to remote servers using the `XdProfileName` parameter, you need to define an authentication profile by using an API access secure client, created in the Citrix Cloud console. For details, see Authentication API.
- You must have permissions to create and delete machine accounts in Active Directory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- We recommend that you automate the PowerShell script with Windows Task Scheduler. For details, see Create an automated task using Windows Task Scheduler.
- If you want the script to write information (for example, failures and actions) to the Windows Event Log, you need to first specify a source name using the `New-EventLog` cmdlet. For example, `New-EventLog -LogName Application –Source <sourceName>`. You can then view the events in the **Application** pane of Windows Event Viewer.
- If errors occurred during execution of the script, execute the script manually and then troubleshoot problems by performing script checks.

Authentication API

Before you run the script, you need to define an authentication profile by using an API access secure client. You must create a secure client using the same account under which the script will run.

The secure client must have the following permissions:

- Create and delete machines using MCS.
- Edit machine catalogs (to add and remove machines).
- Edit delivery groups (to add and remove machines).

When you create a secure client, make sure that your account has the permissions above because the secure client automatically inherits the permissions from your current account.

To create a secure client, complete these steps:

1. Sign in to Citrix Cloud™ and then navigate to **Identity and Access Management > API Access**.
2. Type the name for your secure client and then click **Create Client**.

To authenticate to remote servers, use the `Set-XDCredentials` PowerShell command. For example:

- `Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>`

Create an automated task using Windows Task Scheduler

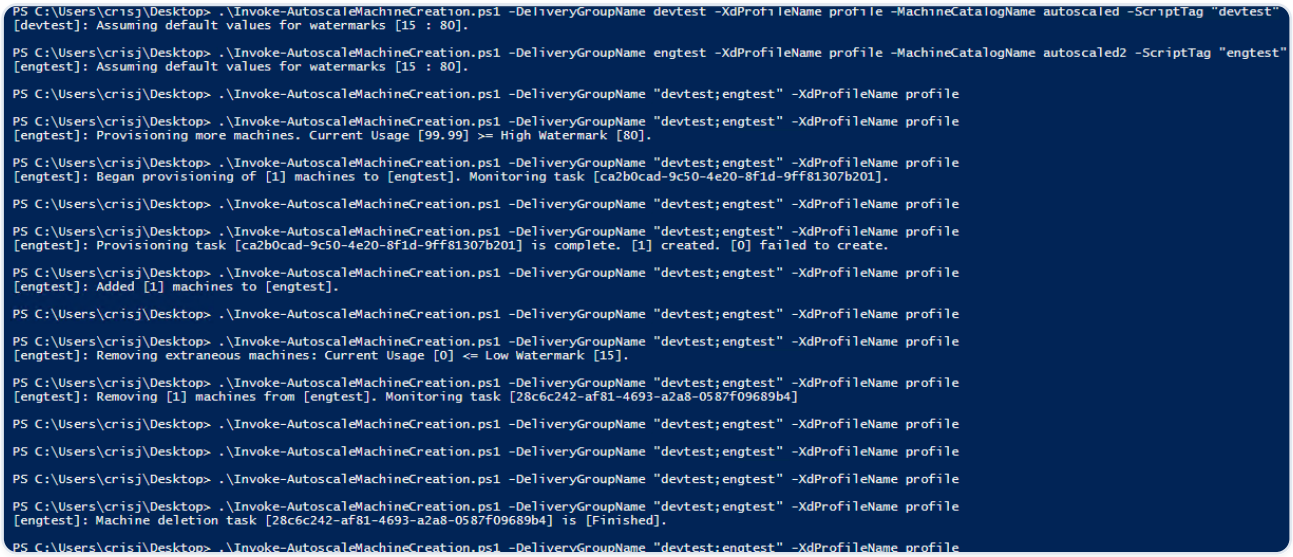
You can automate the PowerShell script with Windows Task Scheduler. Doing so lets the script run automatically at certain intervals or when certain conditions are met. To execute this script with Windows Task Scheduler, make sure to select **Do not start a new instance** on the **Create Task >**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Settings tab. Doing so prevents the Windows Task Scheduler from running a new instance of the script if the script is already running.

Script execution example

See below for an example of executing the script. Note that the script file is invoked multiple times. In this example, to simulate the load, one session is launched and then terminated.



Troubleshooting checklist for the script

The script writes information (for example, errors and actions) to the Windows Event Log. The information helps you troubleshoot issues you experience when executing the script. It might be helpful to keep the following troubleshooting checklist in mind:

- Failure to communicate with remote servers. Possible actions:
  - Verify your connection to the server.
  - Verify that the API key you use is valid.
- Failure to create machines. Possible actions:
  - Verify that the user account running the script has sufficient permissions to create user accounts in the domain.
  - Verify that the user who created the API key has sufficient permissions to use MCS to provision machines.
  - Verify the validity of the machine catalog (that is, its image still exists and is in good state).
- Failure to add machines to a machine catalog or a delivery group. Possible action:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Verify that the user who created the API key has sufficient permissions to add and remove machines to and from machine catalogs and delivery groups.

Autoscale™ plug-in

Autoscale plug-in is a plug-in model where you can take direct action on the power management of VMs. You can deviate from the standard Autoscale settings related to the power management of VMs and instead have different settings for different scenarios. Currently, the plug-ins that you can use are:

- Autoscale holiday plug-in
- Intelligent Autoscale schedules plug-in

Autoscale holiday plug-in

You can use the Autoscale holiday plug-in to handle different settings for holidays. For example, on weekdays, you want most of the VMs to be powered on. However, by default (without the plug-in), the weekday schedule is still applied on public holidays. To handle this scenario, the plug-in allows VMs to be powered off on specified holiday dates.

Create custom holiday schedules using Studio

Use Studio to create custom schedules to turn off unused VMs in a delivery group on specific days, like holidays, to reduce unnecessary resource consumption.

NOTE:

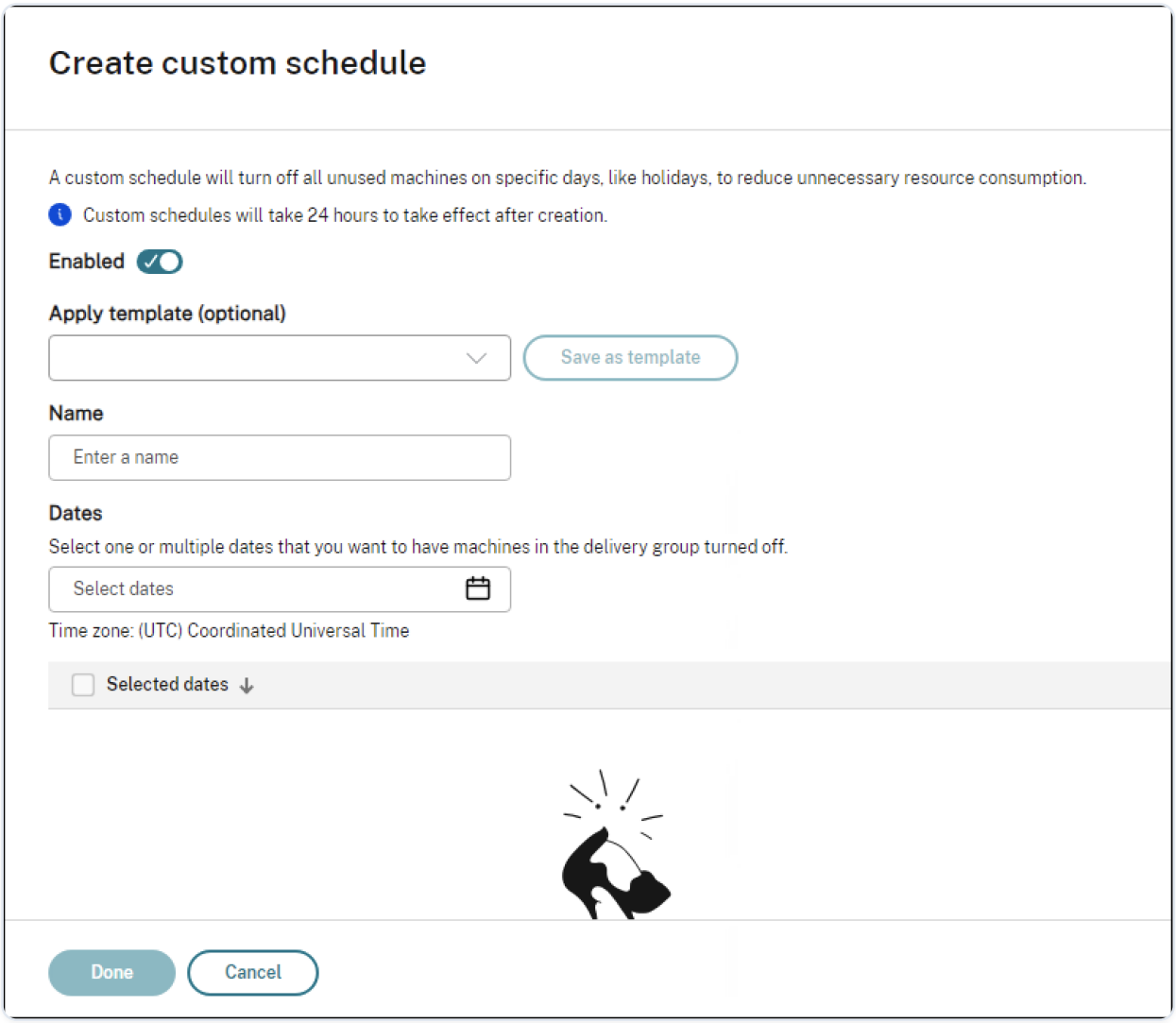
The custom schedule takes effect one day after creation.

To create custom schedules:

1. In Studio, go to **Delivery groups**. Right-click a delivery group and select **Manage Autoscale**.
2. On the **General** page, select **Enable Autoscale**.
3. On the **Schedule** page, click **Create schedule**.
4. Enter a name for the schedule.
5. Select one or multiple dates on which you want the VMs in the delivery group to be turned off.

   If you want to save this schedule as a template for use with other delivery groups, click **Save as template**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Click **Done** to create the custom schedule.

   You must now see the custom schedule created under **Custom** on the **Schedule** page.

To edit a custom schedule:

1. Click the pencil icon under **Actions** for the schedule you want to edit. You can do the following edits:

   - Disable the custom schedule: switch off the **Enable** toggle button.
   - Change or apply a template.
   - Change the name of the schedule.
   - Change the dates of the schedule.

2. Click **Done** to apply the changes.

You can also delete a custom schedule.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Deleting a delivery group also deletes its custom schedules. Saved templates are not deleted.

Configure holiday dates using PowerShell

Associate the Autoscale holiday plug-in with a delivery group and configure the holiday dates so that the plug-in can allow VMs to be powered off on the configured dates. To achieve this, run the following commands:

1. Run `Get-BrokerAutoscalePlugin` to get the UID of the holiday plug-in.

   ```
   (Get-BrokerAutoscalePlugin -Name
   Citrix.AutoscalePlugin.HolidaySchedule).Uid
   ```

   Note the UID value of the `HolidaySchedule` plug-in. Let's assume that the `HolidaySchedule` plug-in has UID 1.

2. Get the UID of the delivery group with which you want to associate the plug-in. For example:

   ```
   $dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
   ```

3. Associate the `HolidaySchedule` plug-in with the delivery group `(-AutoscalePluginUid "<HolidaySchedule plugin UID>")` and specify the required holiday dates. For example:

   ```
   New-BrokerAutoscaleGroupPlugin -Name "Company Holidays"
   -DesktopGroupUid $dgUid -AutoscalePluginUid 1 -Configuration
   '{"Holidays":["2024-11-28","2024-11-29","2024-12-25"]}'
   ```

   Note the UID of the `AutoscaleGroupPlugin` created (the association between the plug-in and the delivery group).

   NOTE:

   The name for the association must be unique among the associations for a given delivery group. For example, there can only be one association called "Company Holidays" for one delivery group, but one or more other delivery groups might also have associations called "Company Holidays".

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CHANGE THE HOLIDAY DATES

You can change the specified holiday dates using the `Set-BrokerAutoscaleGroupPlugin` PowerShell commands and specifying the UID of the `AutoscaleGroupPlugin`. For example, let's assume that the `AutoscaleGroupPlugin` has UID 2.

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"Holidays":
["2024-11-28","2024-11-29"]}'
```

IMPORTANT CONSIDERATIONS

Consider the following when working with the Autoscale holiday plug-in:

- When the Autoscale holiday plug-in is active, all VDAs are off, and the system doesn't operate at a reduced capacity. Any new launch requests are processed, however user might experience a delay due to the VDA being prepared for launch.
- The delivery group must have a timezone specified.
- The date format must be "yyyy-mm-dd".
- Schedule overrides (overrides a standard Autoscale setting) are generated a day in advance at 22:00 on the previous day. After 22:00 it's not possible to add, remove, or change any schedule override for the following day.
- The same Autoscale plug-in can be associated with multiple delivery groups. Run the `New-BrokerAutoscaleGroupPlugin` for each delivery group, and then configure the holidays required for that group.
- The latest `Set-BrokerAutoscalePlugin -Configuration` command overwrites all existing holidays with the new holidays specified.

Intelligent Autoscale schedules plug-in

Intelligent Autoscale is a data driven Autoscale feature with minimum administrative settings that allows you to configure the performance target of a delivery group. The performance target value ranges from 1 to 99 and the value specifies a target balance between user experience and cost:

- A low value prioritizes cost savings.
- A high value prioritizes user experience.

The performance target, combined with historical usage data, calculates an optimal buffer capacity (the number of VMs to be powered on) for each 30-minute block of a day. Therefore, 48 optimal buffer capacities are computed at the start of each day.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The optimal buffer capacity replaces peak/off-peak buffer capacity and pool size to manage available machines.

The historical usage data are used to calculate the optimal buffer capacity are:

- The customer's logon rate in users per minute
- The average VM power-on time, in minutes
- The average VM density, in users per VM.

Prerequisites

Following are the requirements for the Intelligent Autoscale to be enabled:

- The delivery group must be a shared delivery group.
- The delivery group must be Autoscale enabled.
- The delivery group must have at least 90 days worth of historical data before configuring the intelligent Autoscale for a desktop group. You can increase the `ConnectionLogLifetimeHours` from 48 hours to 90 days by using the command:

  ```
  Set-BrokerServiceConfigurationData Logging.ConnectionLogLifetimeHours
  -SettingValue 2160.
  ```

Important considerations

- The delivery group must have a timezone specified.
- Schedule overrides are generated a day in advance at 22:00 on the previous day. After 22:00 it's not possible to add, remove, or change any schedule override for the following day.
- The same Autoscale plug-in can be associated with multiple delivery groups. Run the `New-BrokerAutoscaleGroupPlugin` for each delivery group, and then configure the performance target required for that group.
- The latest `Set-BrokerAutoscalePlugin -Configuration` command overwrites all existing holidays with the new holidays specified.

Configure performance target

Associate the `IntelligentAutoscaleSchedules` plug-in with a delivery group and configure performance target so that the performance target combined with historical usage data can calculate an optimal buffer capacity for each 30-minute block of a day. To achieve this, run the following commands:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Run `Get-BrokerAutoscalePlugin` to get the UID of the Intelligent Autoscale plug-in. Note the UID value of the `IntelligentAutoscaleSchedules` plug-in.

   ```
   (Get-BrokerAutoscalePlugin -Name
   Citrix.AutoscalePlugin.IntelligentAutoscaleSchedules).Uid
   ```

   Let's assume that the `IntelligentAutoscaleSchedules` plug-in has UID 2.

2. Get the UID of the delivery group with which you want to associate the plug-in. For example:

   ```
   $dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
   ```

3. Associate the `IntelligentAutoscaleSchedules` plug-in with the delivery group (`-AutoscalePluginUid "<IntelligentAutoscaleSchedules value>"`) and specify the performance target value.

   ```
   New-BrokerAutoscaleGroupPlugin -DesktopGroupUid $dgUid
   -AutoscalePluginUid 2 -Configuration '{"PerformanceTarget":70}'
   ```

4. Note the UID of the `AutoscaleGroupPlugin` created (the association between the plug-in and the delivery group).

Update performance target value

You can update the specified performance target value using the `Set-BrokerAutoscaleGroupPlugin` PowerShell command and specifying the UID of the `AutoscaleGroupPlugin`. For example, let's assume that the AutoscaleGroupPlugin has UID 2.

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"PerformanceTarget":70}'
```

Configure Autoscale Group plug-in auto-approval

To allow schedule override (overrides a standard Autoscale setting) configure the following two properties in the `BrokerAutoscaleGroupPlugin`:

- `AutoApprove`
  - If `True`: Indicates that any schedule override produced by the plug-in is automatically accepted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - If `False`: The schedule is only accepted if the target date is on or before the date specified in ApprovedUntil properties.

  If `AutoApprove` is `False` and the `ApprovedUntil` date is not set, or is in the past, then any schedule override produced is discarded without being used.

- `ApprovedUntil`:

    - If `AutoApprove` is `False`, and you specify `ApprovedUntil` date, then the schedule override produced by the plug-in is automatically accepted as the schedule for the target date.

For example, let's assume that the `AutoscaleGroupPlugin` has UID 2.

- To enable auto-approval for that desktop group:

```
Set-BrokerAutoscaleGroupPlugin 2 -AutoApprove $true
```

- To enable auto approval until some date in the future:

```
Set-BrokerAutoscaleGroupPlugin 2 -ApprovedUntil "2025-01-01"
```

User logoff notifications

IMPORTANT:

This feature is available only in the Autoscale™ user interface for multi-session app-based delivery groups.

To better achieve cost savings, Autoscale lets you force log off lingering sessions. It does so by letting you send a custom notification to the users and specify a grace period after which the sessions are force logged off. This is done only for machines in drain state and not for all powered-on machines. To avoid potential data loss caused by forcing user logoffs, you can instead configure this feature to only send logoff reminders without forcing user logoff.

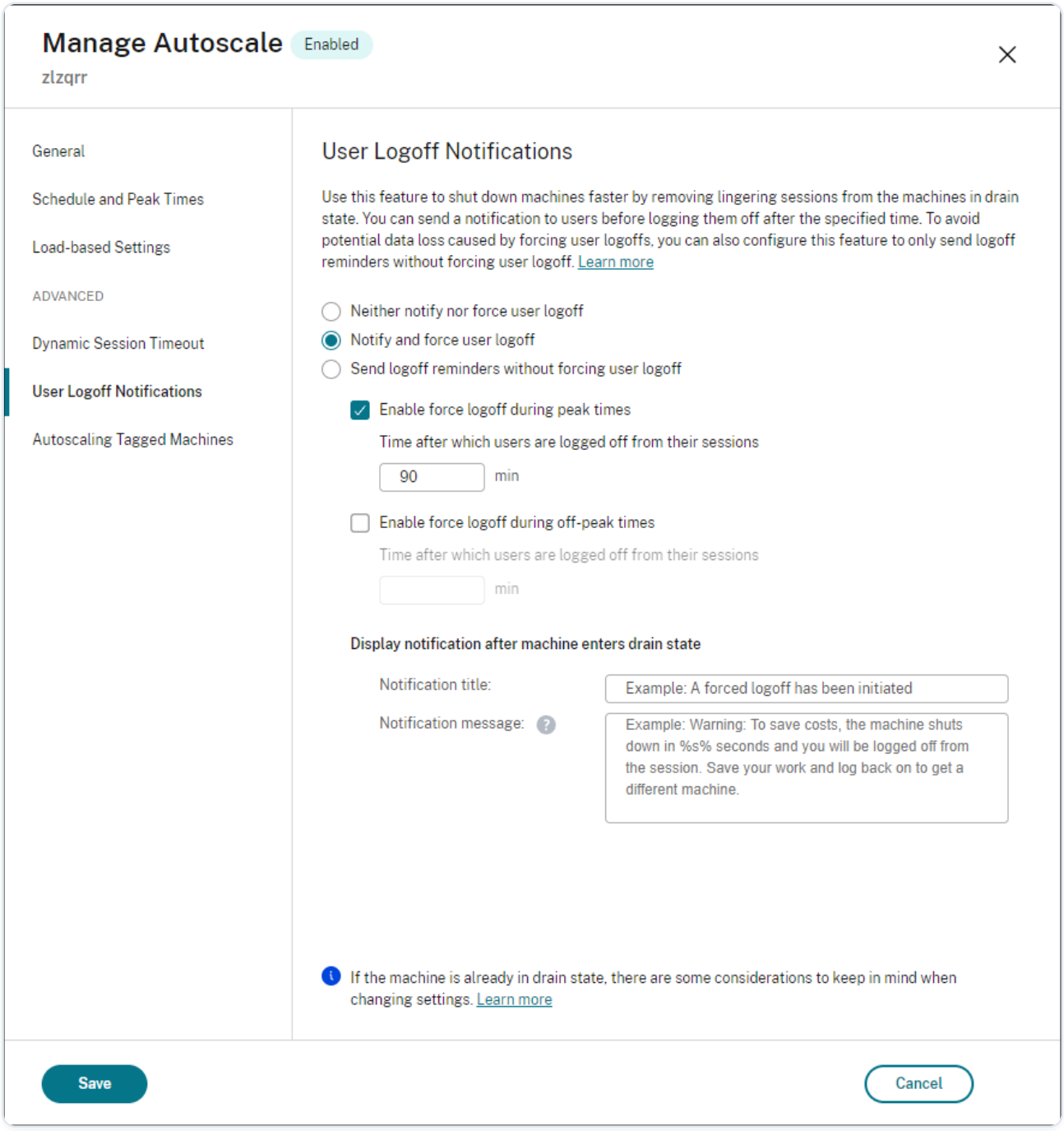
You have the following options:

- **Notify and force user logoff**
- **Send logoff reminders without forcing user logoff**
- **Neither notify nor force user logoff**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Notify and force user logoff

If selected, Autoscale logs off users from their sessions after the times specified below.



Enable force logoff during peak times. If selected, Autoscale logs off those users from their sessions during peak times when the specified time elapses.

Enable force logoff during off-peak times. If selected, Autoscale logs off those users from their sessions during off-peak times when the specified time elapses.

Display notification after machine enters drain state. Lets you send notifications to users after their machine enters drain state.

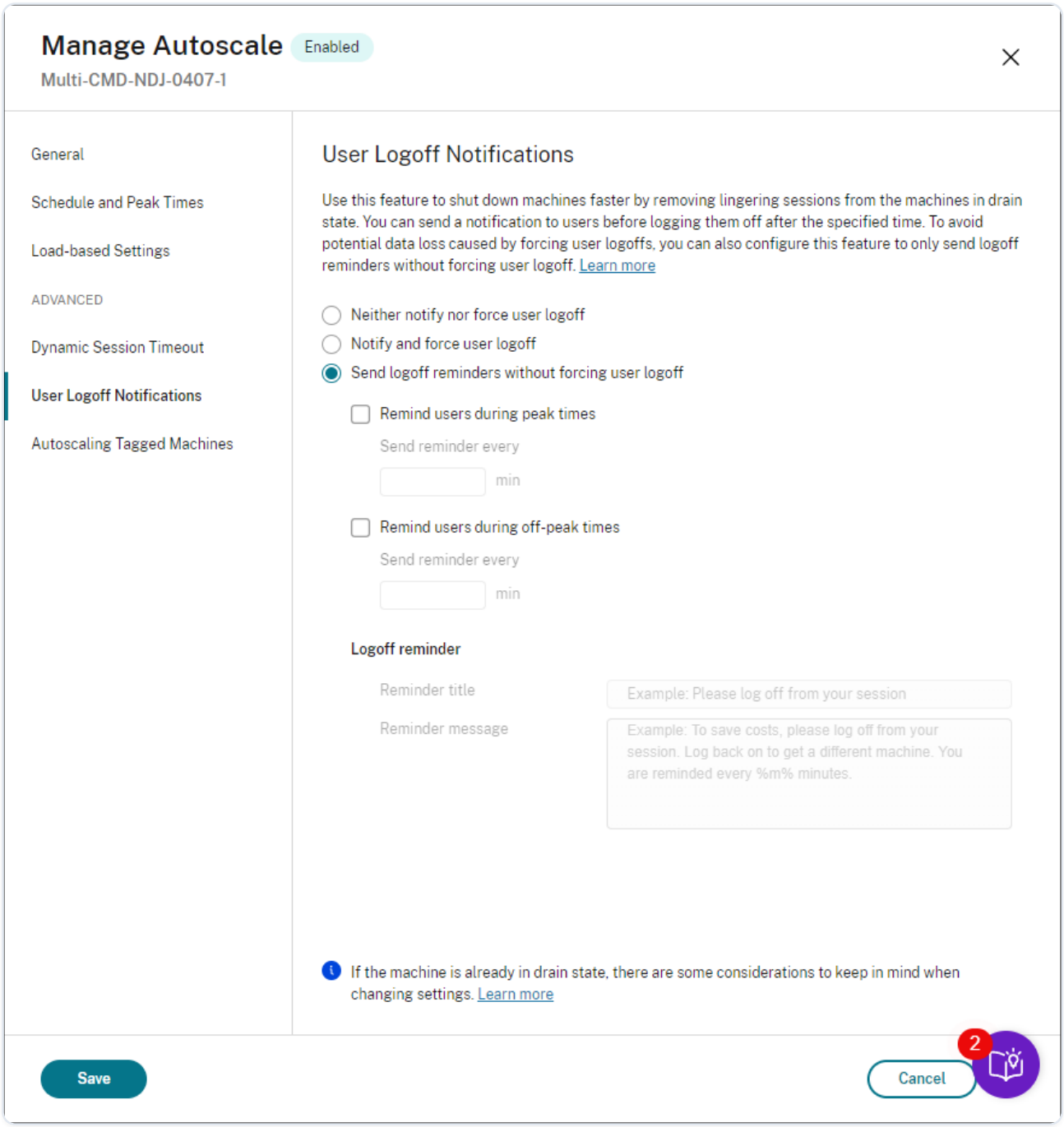
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Notification title**. Lets you specify a title of the notification to be sent to users. Example: `A forced logoff has been initiated.`
- **Notification message**. Lets you specify the content of the notification to be sent to users. You can use %s% or %m% as variables to indicate the specified time in the message. To express the time in seconds, use %s%. To express the time in minutes, use %m%. Example: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`

Send logoff reminders without forcing user logoff

If selected, users will receive a reminder to log off from their machine after it has entered drain state. This reminder can be configured to be sent at the interval specified below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Remind users during peak times. If selected, users receive a reminder to log off from their sessions during peak times every X minutes (X denotes the specified time).

Remind users during off-peak times. If selected, users receive a reminder to log off from their sessions during off-peak times every X minutes (X denotes the specified time).

Logoff reminder. Lets you configure the reminder sent to users after their machine enters drain state.

- **Reminder title**. Lets you specify a title for the reminder to be sent to users. Example: `Please log off from your session`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Reminder message**. Lets you specify a message to be sent to users. Example: `Please log off from your session and log back on to save costs`.

Neither notify nor force user logoff

If selected, Autoscale neither forces users to log off from machines in drain state nor notifies users to manually switch to a different machine.

Considerations

If the machine is already in drain state, consider the following when changing settings:

- If you change the setting from **Send logoff reminders without forcing user logoff** to **Notify and force user logoff**, the new setting takes effect immediately.
- If you change the setting from **Notify and force user logoff** to **Send logoff reminders without forcing user logoff**, the new setting does not take effect until the next time the machine enters drain state. The user is still forced to log off.

Analyze the effectiveness of Autoscale™ settings

To use this feature, enable the toggle **Autoscale Insights** in **DaaS > Home > Preview features**. It might take about 15 minutes for **Autoscale Insights** to show up after enabling it.

You can analyze the effectiveness of the Autoscale settings based on machine usage from the previous week. Through the analysis, you can gain these insights into the effectiveness of Autoscale settings:

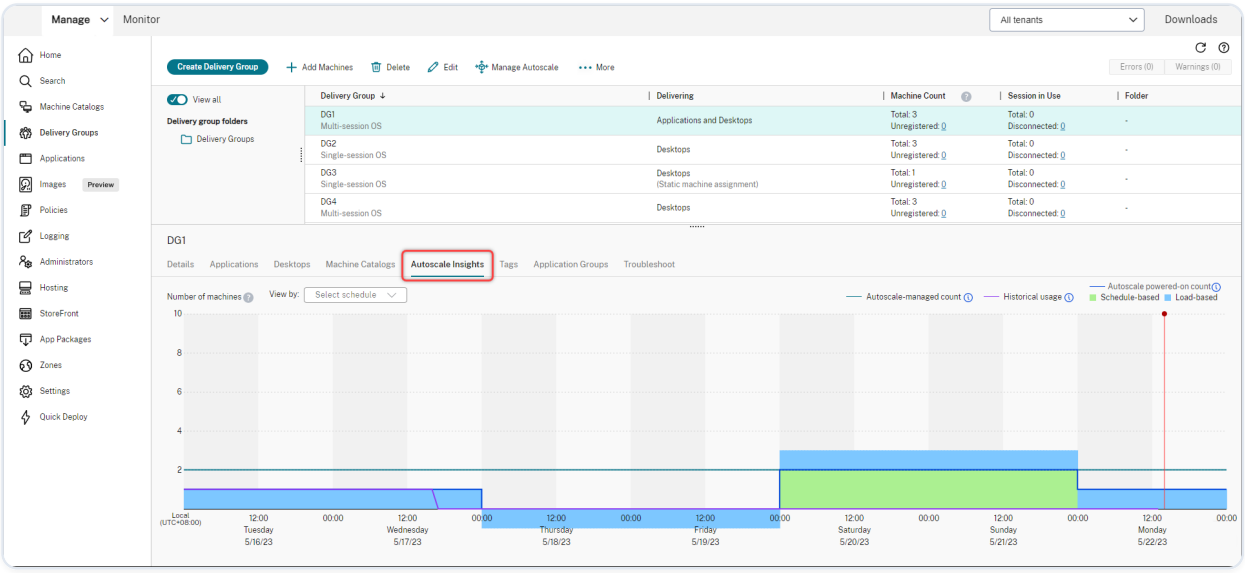
- Identify financial waste resulting from over-provisioning.
- Determine whether the user experience is negatively impacted due to under-provisioning.
- Ensure that the capacity provisioned is properly aligned with the machine usage.

To achieve this goal, follow these steps:

1. Select an Autoscale-enabled delivery group.
2. In the bottom pane, click the **Autoscale Insights** tab.

   The following graph appears, showing the comparison between machine usage data from the previous week and the number of machines to be powered on based on Autoscale settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



* The red vertical line identifies the current time.

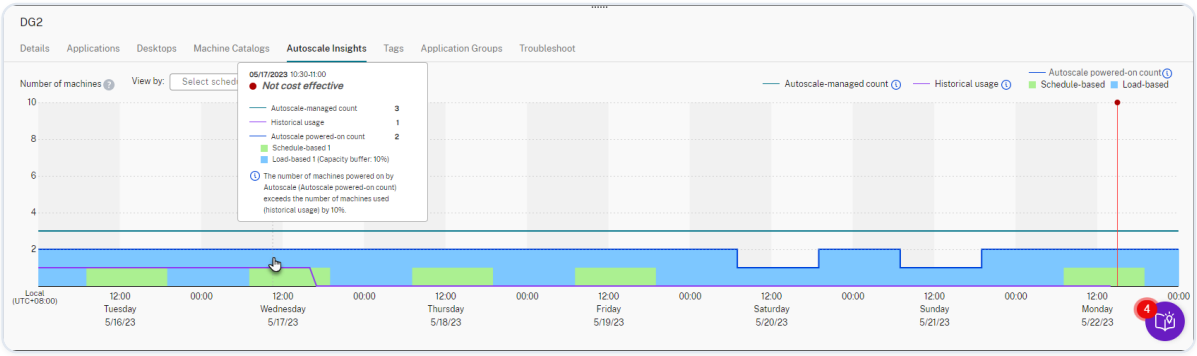
The following table provides descriptions of the metrics shown in this graph.

METRIC	DESCRIPTION
Autoscale-managed count	Total number of machines managed by Autoscale. Autoscale-managed count = Total number of machines in the delivery group – Number of machines in maintenance mode – Number of machines not tagged for Autoscale (If tagged Autoscale feature is enabled).
Autoscale powered-on count	Total number of machines powered on by Autoscale. Autoscale powered-on count = Schedule-based machine count + Load-based machine count.
Historical usage	Number of machines that were delivered to users.
Schedule-based	Number of machines that are powered on based on the Autoscale schedule-based settings (**Note:** Schedule-based settings don't apply to delivery groups of the static single-session OS type).
Load-based	Number of machines that are powered on based on the Autoscale load-based settings.

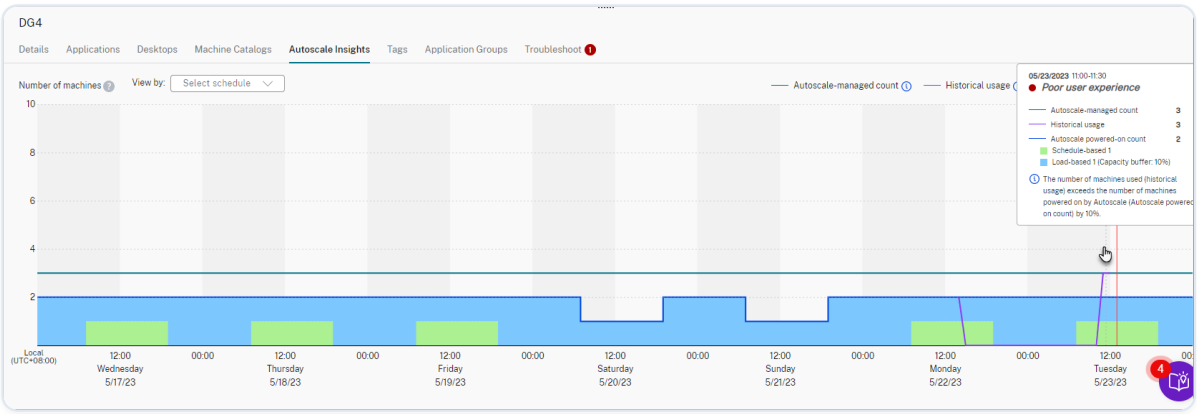
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. To check the effectiveness of Autoscale settings at a specific time slot, hover your mouse over that slot on the graph. An information box appears, showing the comparison results and detailed machine counts:

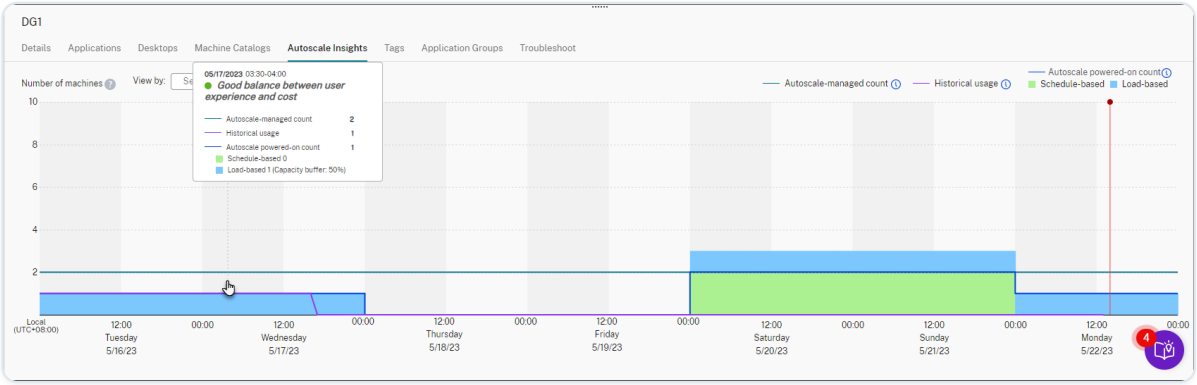
   - **Not cost effective**. The historical usage is less than 90% of the Autoscale settings (Autoscale powered-on count). As a result, wasted capacity might exist.



   - **Poor user experience**. The historical usage is more than 110% of the Autoscale settings (Autoscale powered-on count). As a result, users might experience longer wait times for machines to power on.

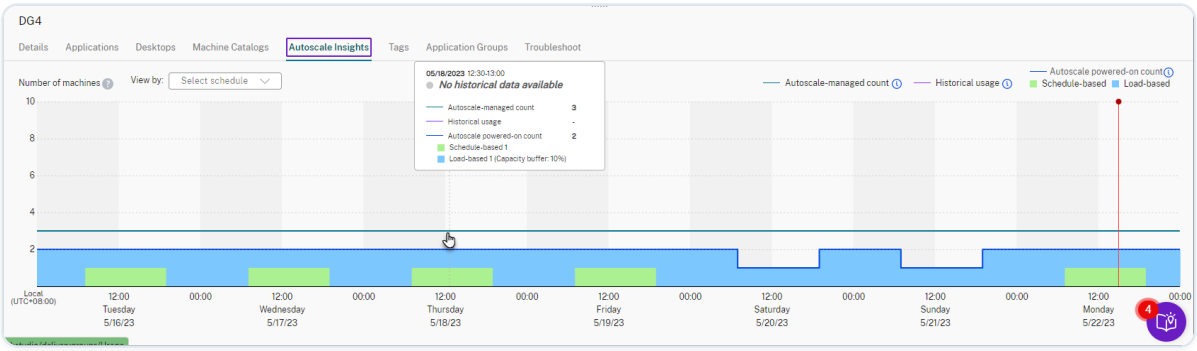


   - **Good balance between user experience and cost**. The difference between the historical usage and the Autoscale settings (Autoscale powered-on count) is less than 10%. The Autoscale settings are aligned with the historical usage.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **No historical data available**. No historical data is available. Possible causes include that Autoscale was enabled for the delivery group less than a week ago.



4. To highlight a date range based on an Autoscale schedule, select the schedule from the **View by** field.
5. Based on your analysis, adjust the Autoscale settings. For more information, see Schedule-based and load-based settings.

Broker PowerShell SDK commands

You can configure Autoscale for delivery groups using the Broker PowerShell SDK. To configure Autoscale using PowerShell commands, you must use Remote PowerShell SDK version 7.21.0.12 or later. For more information about the Remote PowerShell SDK, see SDKs and APIs.

Set-BrokerDesktopGroup

Disables or enables an existing BrokerDesktopGroup or alters its settings

For more information about this cmdlet, see `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`.

EXAMPLES

See the following examples for details about how to use the PowerShell cmdlets.

Enable Autoscale™:

- Suppose you want to enable Autoscale for the delivery group whose name is "MyDesktop." Use the `Set-BrokerDesktopGroup` PowerShell command. For example:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

Configure the capacity buffer separately for peak and off-peak times:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Suppose you want to set the capacity buffer to 20% for peak times and 10% for off-peak times for a delivery group whose name is "MyDesktop." Use the `Set-BrokerDesktopGroup` PowerShell command. For example:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

Configure the *when disconnected timeout* setting:

- Suppose you want to set the **when disconnected timeout** value to 60 minutes for peak times and 30 minutes for off-peak times for a delivery group whose name is "MyDesktop." Use the `Set-BrokerDesktopGroup` PowerShell command. For example:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

Configure the *when logged off timeout* setting:

- Suppose you want to set the **when logged off timeout** value to 60 minutes for peak times and 30 minutes for off-peak times for a delivery group whose name is "MyDesktop." Use the `Set-BrokerDesktopGroup` PowerShell command. For example:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

Configure the *power-off delay* setting:

- Suppose you want to set the power-off delay to 15 minutes for a delivery group whose name is "MyDesktop." Use the `Set-BrokerDesktopGroup` PowerShell command. For example:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

Configure a time period during which the power-off delay does not take effect:

- Suppose you want the power-off delay to take effect until 30 minutes have elapsed for a delivery group whose name is "MyDesktop." Use the `Set-BrokerDesktopGroup` PowerShell command. For example:
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`.

Configure the *machine instance cost* setting:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Suppose you want to set the machine instance cost per hour to 0.2 dollars for a delivery group whose name is "MyDesktop." Use the `Set-BrokerDesktopGroup` PowerShell command. For example:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

Exclude maintenance mode VMs from the autoscale pool:

- Consider a delivery group with 10 machines, out of which 2 machines are in maintenance mode. Autoscale buffer capacity is set to 50%. Suppose if you want to exclude the VMs in maintenance mode from the autoscale pool, then set `PoolSizeExcludesMaintenanceMode` to `True`. Autoscale then starts 4 machines as the 2 machines in maintenance mode are not included in the machine pool. Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

  ```
  PS C:\> Set-BrokerDesktopGroup -PoolSizeExcludesMaintenanceMode $true
  ```

  The default value for `PoolSizeExcludesMaintenanceMode` for the single-session delivery groups is `False`.

  The default value for `PoolSizeExcludesMaintenanceMode` for the multi-session delivery groups is `True`.

New-BrokerPowerTimeScheme

Creates a BrokerPowerTimeScheme for a delivery group. For more information, see `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`.

Example

Suppose you want to create a power time scheme for a delivery group whose UID value is 3. The new scheme covers the weekend, Monday, and Tuesday. The 8:00 AM to 6:30 PM time slot is defined as peak times for the days included in the scheme. For peak times, the pool size (the number of machines kept powered on) is 20. For off-peak times, it is 5. You can use the `Set-BrokerDesktopGroup` PowerShell command. For example:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

Parameters for dynamic session timeouts

The following Broker PowerShell SDK cmdlets have been extended for dynamic session timeouts by supporting multiple new parameters:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Those parameters include:

- **DisconnectPeakIdleSessionAfterSeconds** – Represents the time in seconds after which an idle session is disconnected during peak time. This property has a default value of 0, which indicates the disablement of its associated behavior during peak time. A value greater than 0 enables its behavior for the delivery group during peak time only.
- **DisconnectOffPeakIdleSessionAfterSeconds** - Represents the time in seconds after which an idle session is disconnected during off-peak hours. The default value of this property is 0, which indicates the disablement of its associated behavior during off-peak. A value greater than 0 enables its associated behavior for the delivery group during off-peak hours only.
- **LogoffPeakDisconnectedSessionAfterSeconds** - Represents the time in seconds after which a disconnected session is terminated during peak time. The default value of this property is 0, which indicates the disablement of its associated behavior during peak time. A value greater than 0 enables its associated behavior for the delivery group during peak time only.
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - Represents the time in seconds after which a disconnected session is terminated during off-peak hours. The default value of this property is 0, which indicates the disablement of its associated behavior during off-peak. A value greater than 0 enables its associated behavior for the delivery group during off-peak hours only.

Example

Suppose you want to set the idle session timeout to 3,600 seconds during peak times for a delivery group whose name is "MyDesktop." Use the `Set-BrokerDesktopGroup` PowerShell command. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

Doing that disconnects sessions that have been idle for more than 1 hour in off-peak for the desktop group whose name is "MyDesktop."

Cloud Health Check

NOTE:

Cloud Health Check is integrated into Citrix DaaS. The integration is available as the Run Health Check action in Studio. For more information, see Troubleshoot VDA registration and session launch issues.

Cloud Health Check allows you to run checks that gauge the health and availability of the site and its components. You can run health checks for Virtual Delivery Agents (VDAs), StoreFront™ servers, and Profile Management. VDA health checks identify possible causes for common VDA registration and session launch issues.

If issues are present during the checks, Cloud Health Check provides a detailed report and the actions to fix the issues. Each time Cloud Health Check starts, it checks for the latest version of scripts on the Content Delivery Network (CDN) and automatically downloads the scripts if they do not exist on the local machine. Cloud Health Check always chooses the latest local version of scripts to run health checks.

NOTE:

Cloud Health Check does not update every time it runs.

In a Citrix Cloud™ environment, run Cloud Health Check from a domain-joined machine to run checks on one or more VDAs or StoreFront servers.

NOTE:

You cannot install or run Cloud Health Check on a Cloud Connector.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The log for the Cloud Health Check application is stored in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`. You can use this file for troubleshooting.

View an introduction to Cloud Health Check.



View when to use Cloud Health Check.



Installation

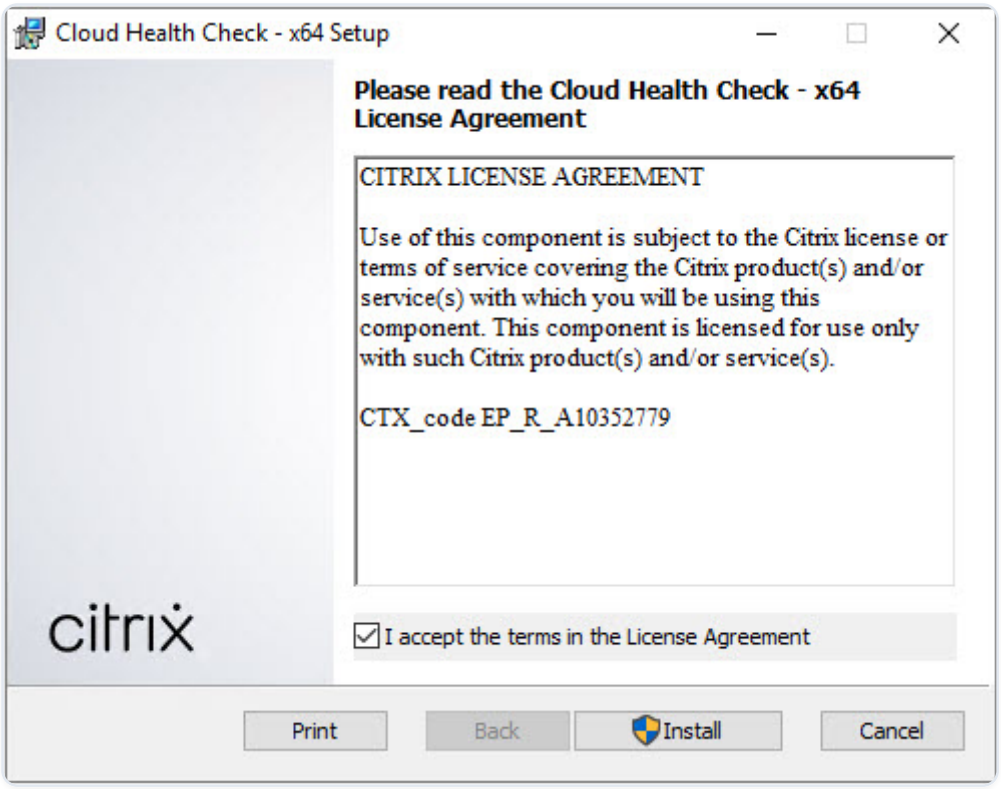
To prepare your environment for installation of Cloud Health Check, you must have a domain-joined Windows machine.

NOTE:

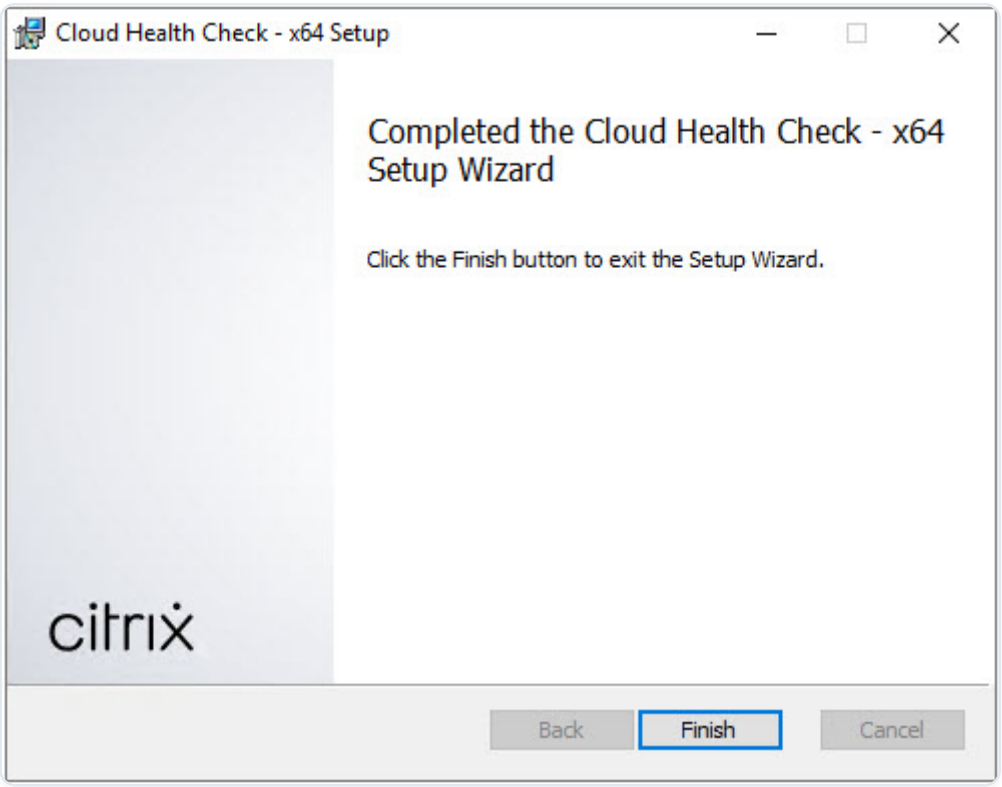
You cannot install or run Cloud Health Check on Cloud Connector.

1. On the domain-joined machine, download the Cloud Health Check installer.
2. Double-click the CloudHealthCheckInstaller_x64.msi file.
3. Click the box to accept the terms.
4. Click Install.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. After installation has completed, click **Finish**.



Permissions and requirements

Permissions:

- To run health checks:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - You must be a member of the domain users group.
    - You must be a full administrator or have a custom role with read-only and **Run Environment Tests** permissions for the site.
    - Set the script execution policy to at least `RemoteSigned` to allow the scripts to run. For example: `Set-ExecutionPolicy RemoteSigned`. **Note:** other script execution permissions can work as well.

- Use **Run as administrator** when launching Cloud Health Check.

For each VDA or StoreFront machine that you run health checks on:

- The OS must be 64-bit.
- The machine must be joined to the same Active Directory domain forest as the health check host.
- Cloud Health Check must be able to communicate with the machine.
- File and printer sharing must be turned on.
- PSRemoting and WinRM must be enabled. The machine must also be running PowerShell 3.0 or later.
- Windows Management Infrastructure (WMI) access must be enabled on the machine.

About health checks

Health check data is stored in folders under `C:\ProgramData\Citrix\TelemetryService\`.

VDA health checks

For registration on the VDA, Cloud Health Check checks:

- VDA software installation
- VDA machine domain membership
- VDA communication port availability
- VDA service status
- Windows firewall configuration
- Communication with Controller
- Time sync with Controller
- VDA registration status

For session launches on VDAs, Cloud Health Check checks:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Session launch communication port availability
- Session launch services status
- Session launch Windows firewall configuration
- VDA Remote Desktop Services Client Access Licenses
- VDA application launch path
- Session launch registry settings
- Citrix Universal™ Injection Driver (CTXUVI) status

For Profile Management on VDAs, Cloud Health Check checks:

- Hypervisor detection
- Provisioning detection
- Citrix Virtual Apps and Desktops™
- Personal vDisk configuration
- User store
- Profile Management Service status detection
- Winlogon.exe hooking test

To run checks on Profile Management, you must install and enable Profile Management on the VDA. For more information on Profile Management configuration checks, see Knowledge Center article CTX132805.

StoreFront health checks

StoreFront checks verify whether:

- Citrix Default Domain service is running
- Citrix Credential Wallet service is running
- The connection from the StoreFront server to Active Directory is port 88
- The connection from the StoreFront server to Active Directory is port 389
- The connection from the StoreFront server to Active Directory is port 464
- The base URL has a valid FQDN
- The correct IP address from the base URL can be retrieved
- The IIS application pool is using .NET 4.0
- The certificate is bound to the SSL port for the host URL

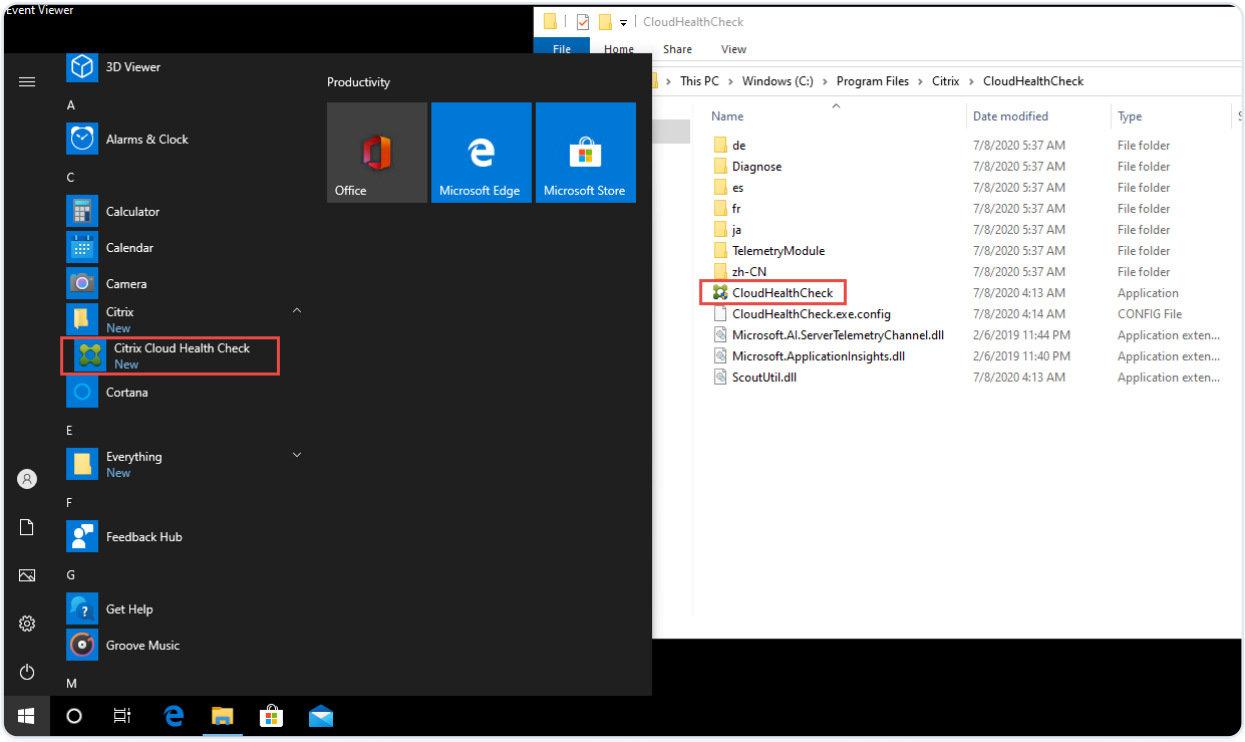
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The certificate chain is complete
- The certificates have expired
- A certificate is expiring within 30 days

Running Cloud Health Check

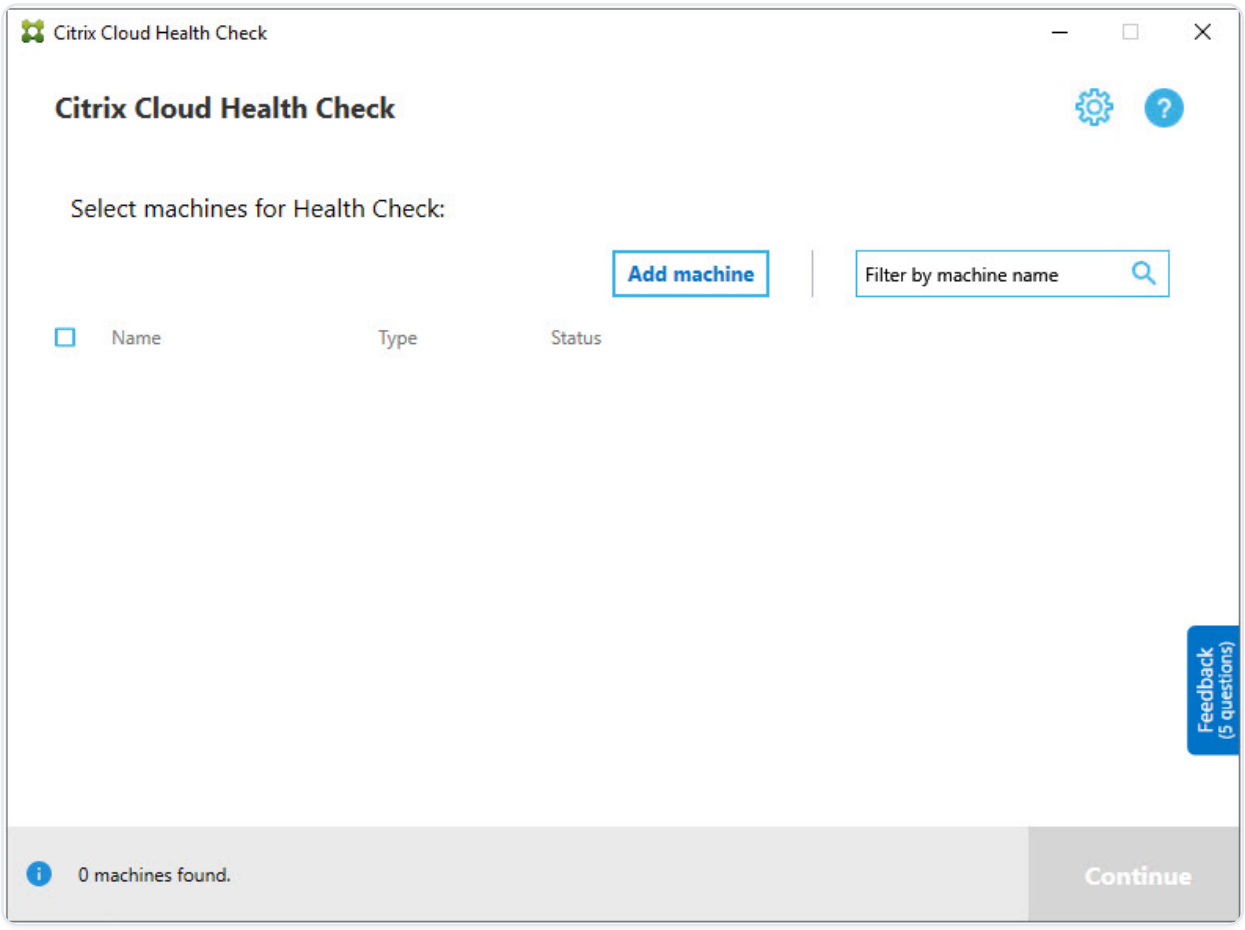
To run Citrix Cloud Health Check:

1. Select **Citrix > Citrix Cloud Health Check** from the machine's Start menu, or run `CloudHealthCheck.exe` in `C:\Program Files\Citrix\CloudHealthCheck`.



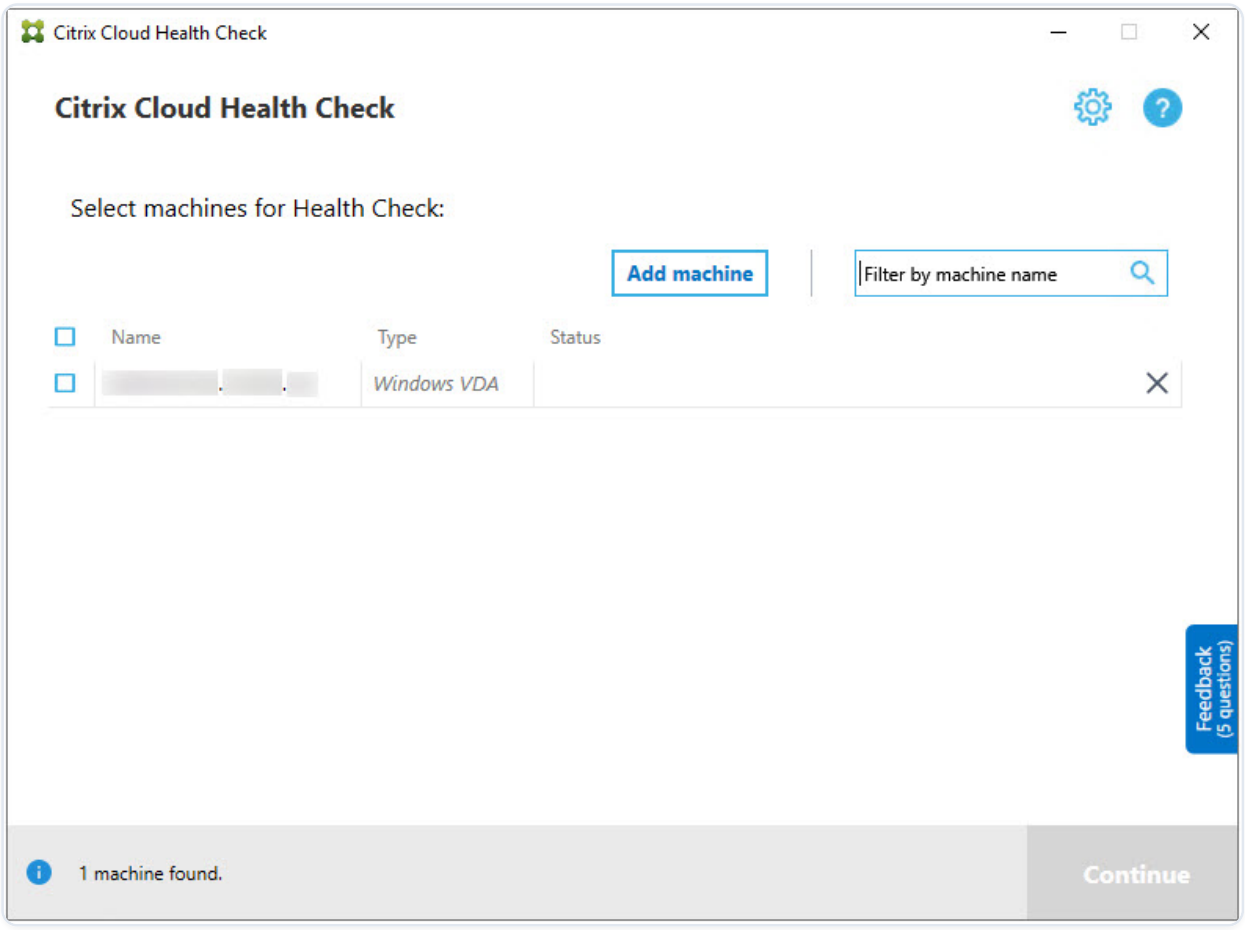
2. On the main Cloud Health Check screen, click **Add machine**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Type the FQDN of the machine you want to add. **Note:** Although entering a DNS alias instead of an FQDN can appear valid, the health checks might fail.
4. Click **Continue**.
5. Repeat to add other machines as needed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. To remove a manually added machine, click the **X** on the right end of the row and confirm the deletion. Repeat to delete other manually added machines.

Cloud Health Check remembers manually added machines until you remove them. When you close and then reopen Cloud Health Check, the manually added machines are still listed at the top of the list.

Import VDA machines

You can import VDA machines in the deployment when running health checks.

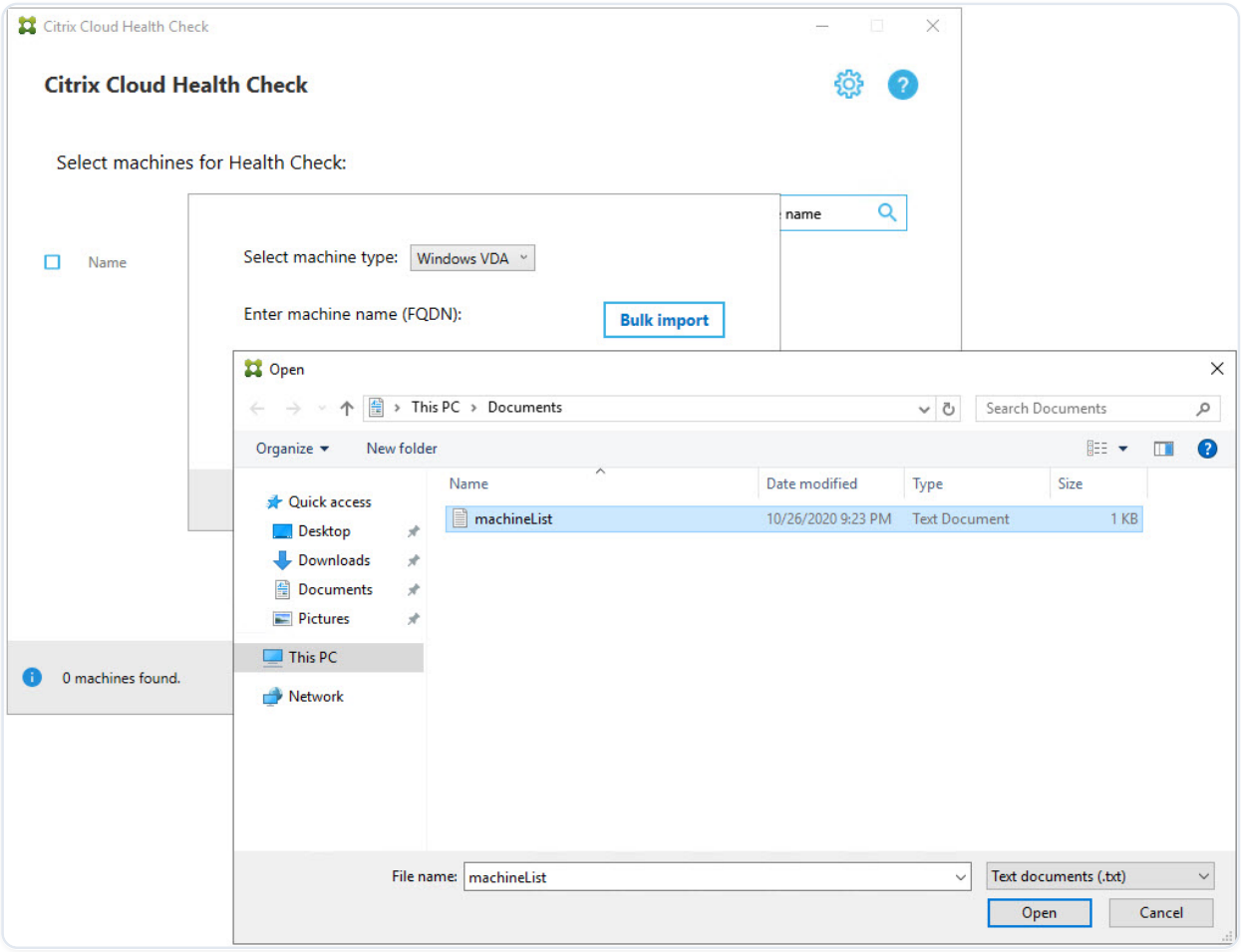
1. On Connector, generate the machine list file with the following PowerShell command. On Connector, you must input Citrix credentials and select the customer in the pop-up dialog.

```
Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
```

1. Copy the machineList.txt file to the domain-joined machine you want to run Cloud Health Check on.
2. On the Cloud Health Check page, click **Add Machine**.
3. Select the Windows VDA machine type.
4. Click **Import VDA machines**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select the machineList.txt file.
6. Click **Open**.



The imported VDA machines are listed on the Cloud Health Check page.

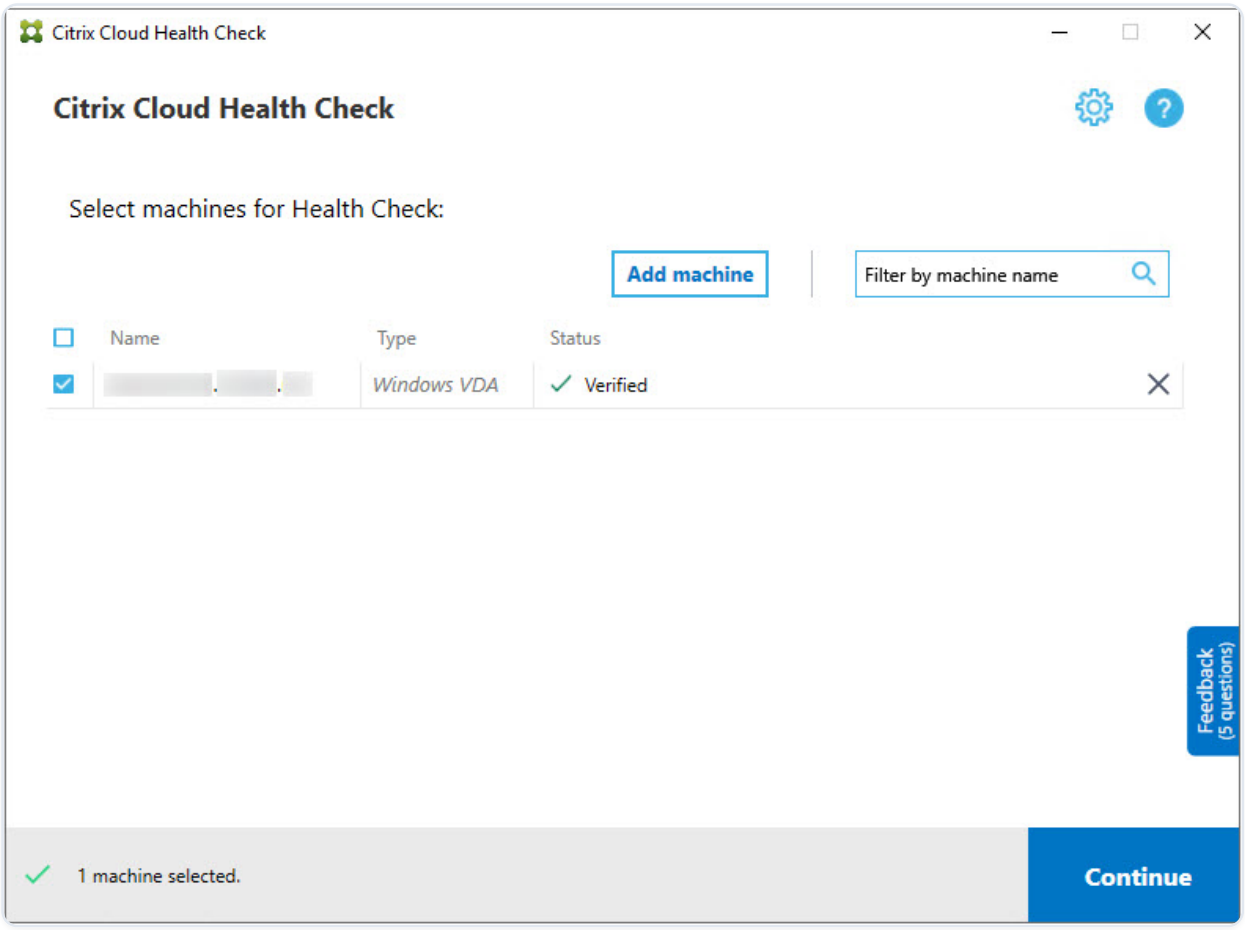
7. Select the check box next to each machine you want to run health checks on.

   Cloud Health Check automatically launches verification tests on each selected machine, making sure it meets the criteria listed in verification tests. If verification fails, a message appears in the **Status** column, and that machine's check box is cleared. You can then:

   - Resolve the issue and then select the machine's check box again. This triggers a retry of the verification tests.
   - Skip that machine by leaving its check box unselected. Health checks are not run for that machine.

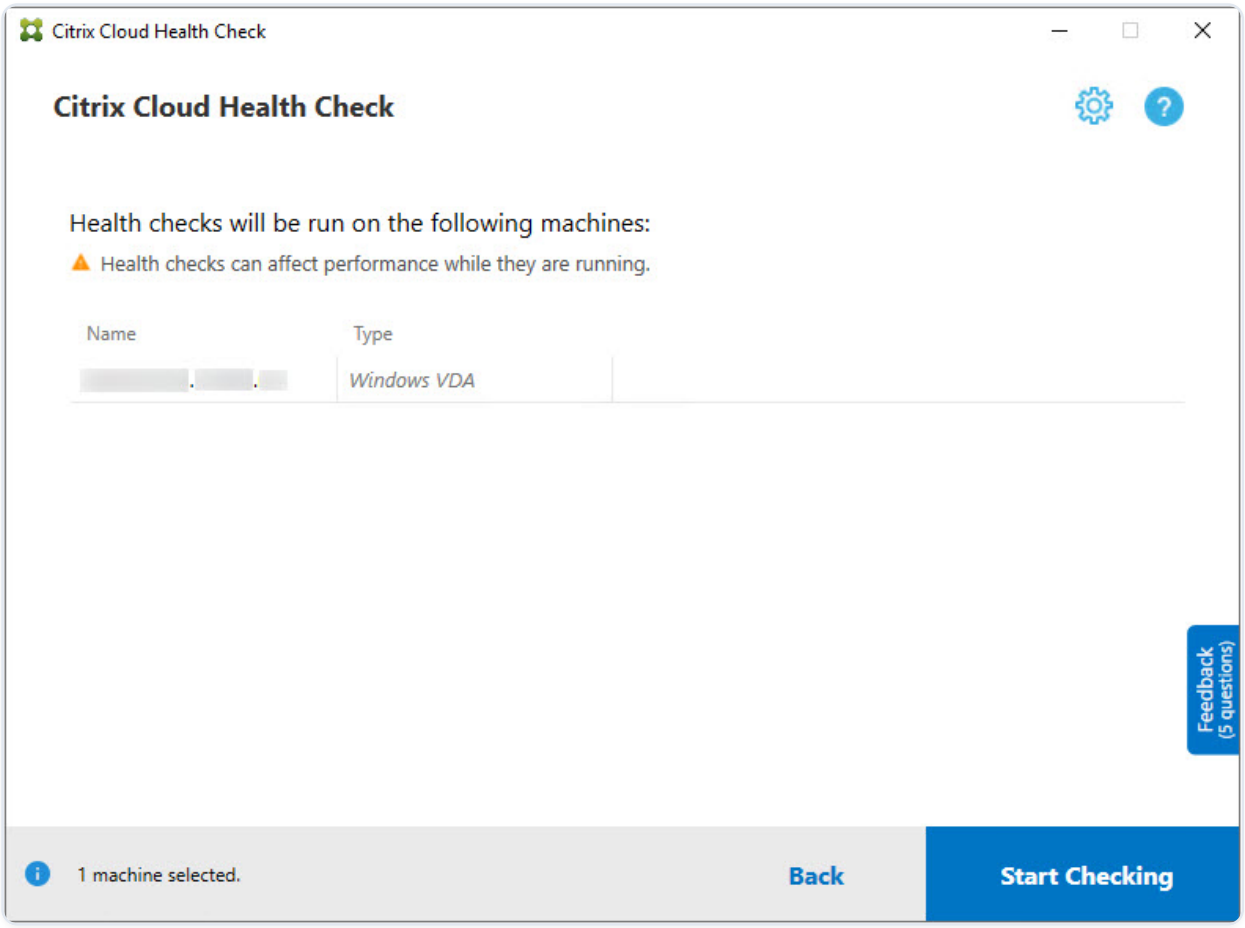
8. When the verification tests are complete, click **Continue**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. Run the health checks on the selected machines. The summary lists the machines where the tests run (the machines you selected that passed the verification tests).
10. Click **Start Checking**.

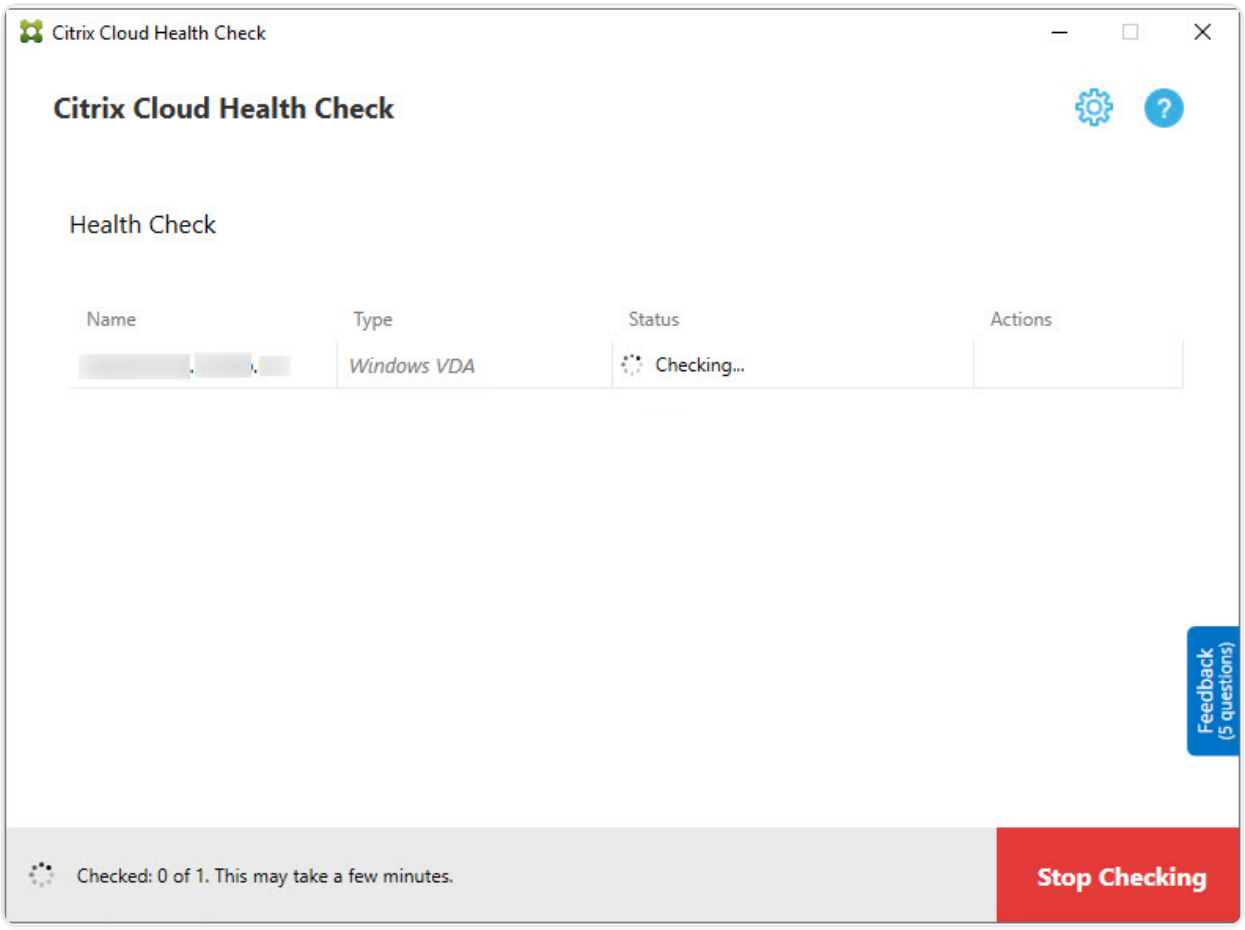
© 1997–2026 Citrix Systems, Inc. All rights reserved.



During and after checking, the **Status** column indicates the current checking state for a machine.

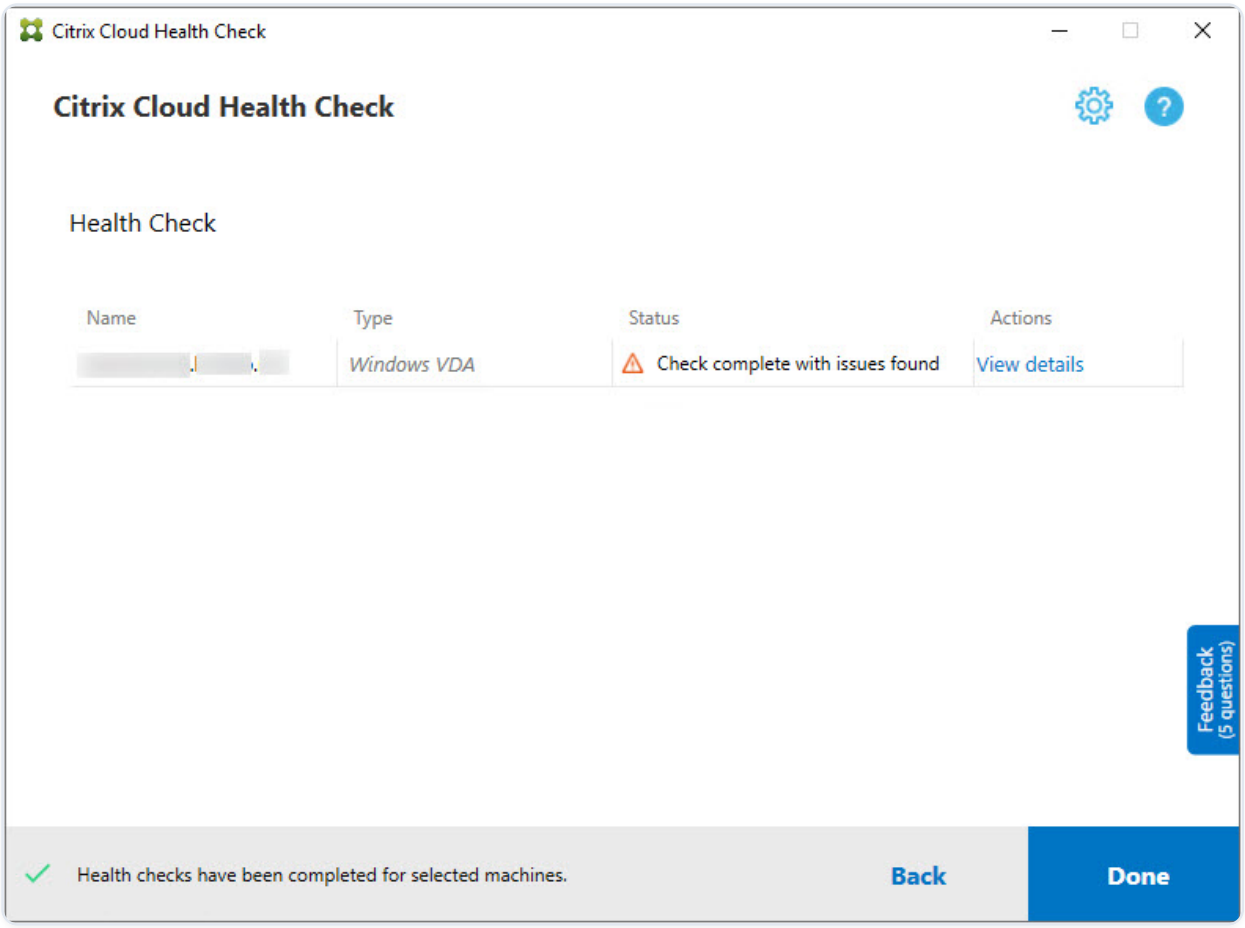
11. To stop all in-progress checks, click **Stop Checking** in the lower right corner of the page. You can't cancel a single machine's health check, you can only cancel the check for all selected machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

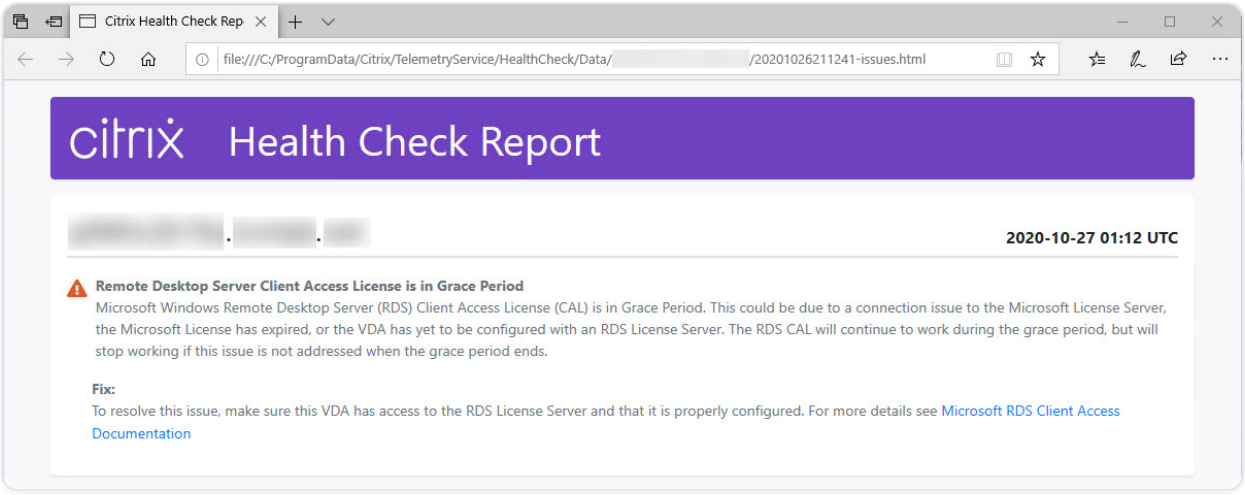


12. When the checks are complete for all selected machines, the **Stop Checking** button in the lower right corner changes to **Done**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

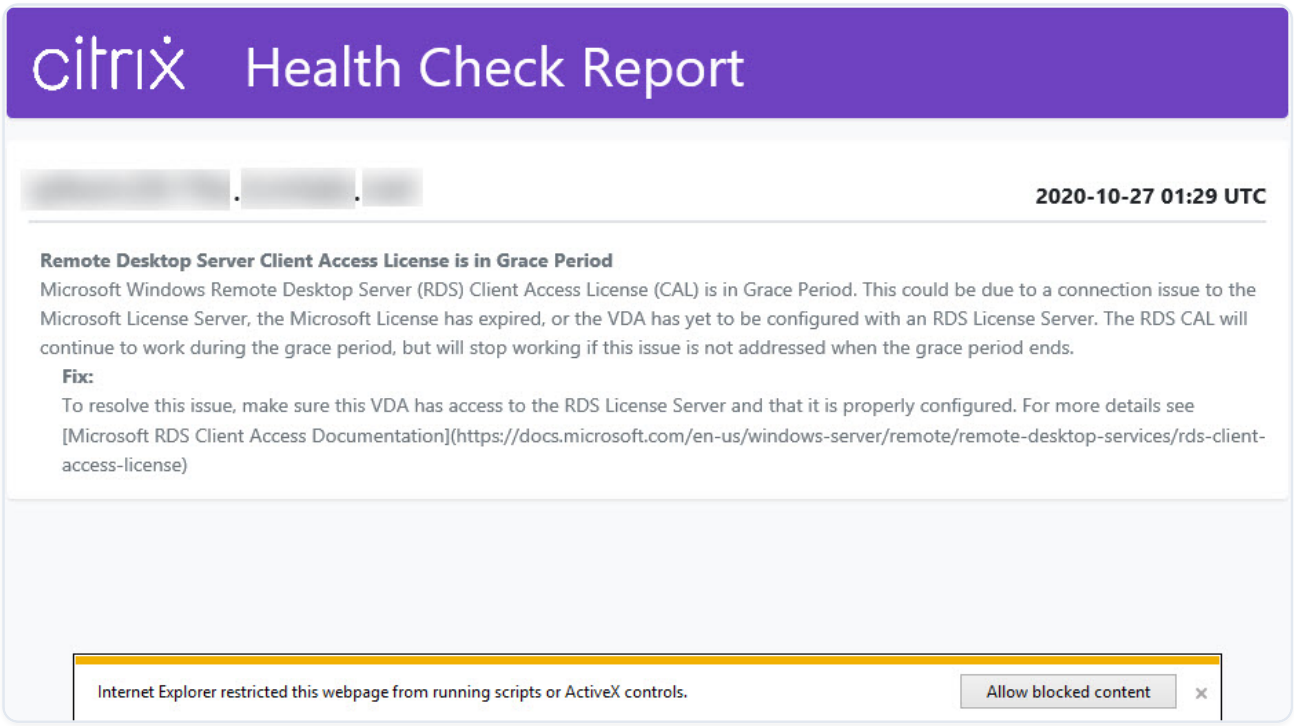


- If a check fails, you can click **Retry** in the **Action** column.
- If a check completes with no issues found, the **Action** column is empty.
- If a check finds issues, click **View Details** to view the results.



If you use Internet Explorer to view the report, you must click **Allow blocked content** to display the hyperlink.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After the check completes for all selected machines, clicking **Back** causes you to lose your check results.

When the checks complete, click **Done** to return to the Cloud Health Check main screen.

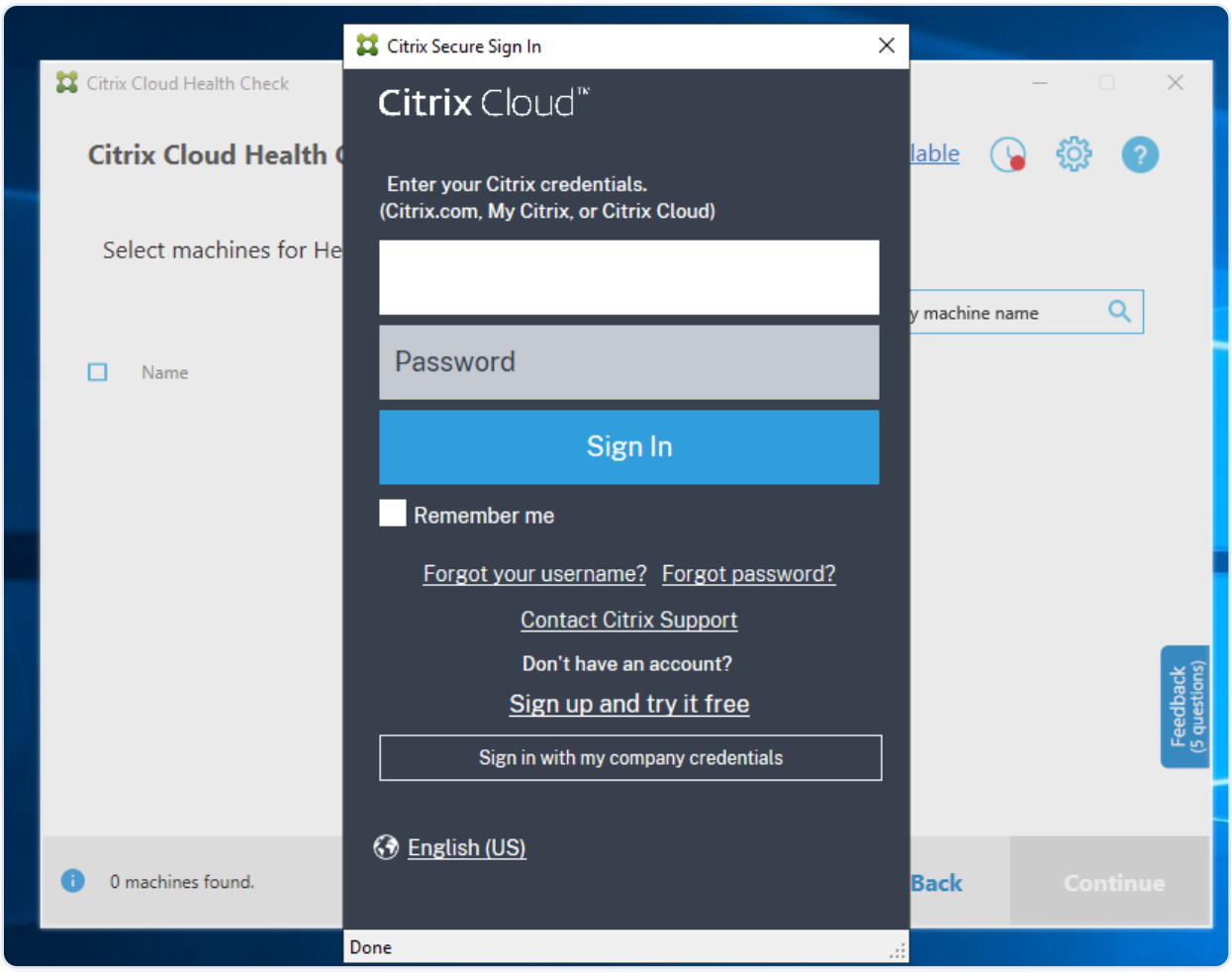
Retrieve VDA machines

Cloud Health Check can automatically detect and retrieve VDAs from your Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployments.

To retrieve your VDAs:

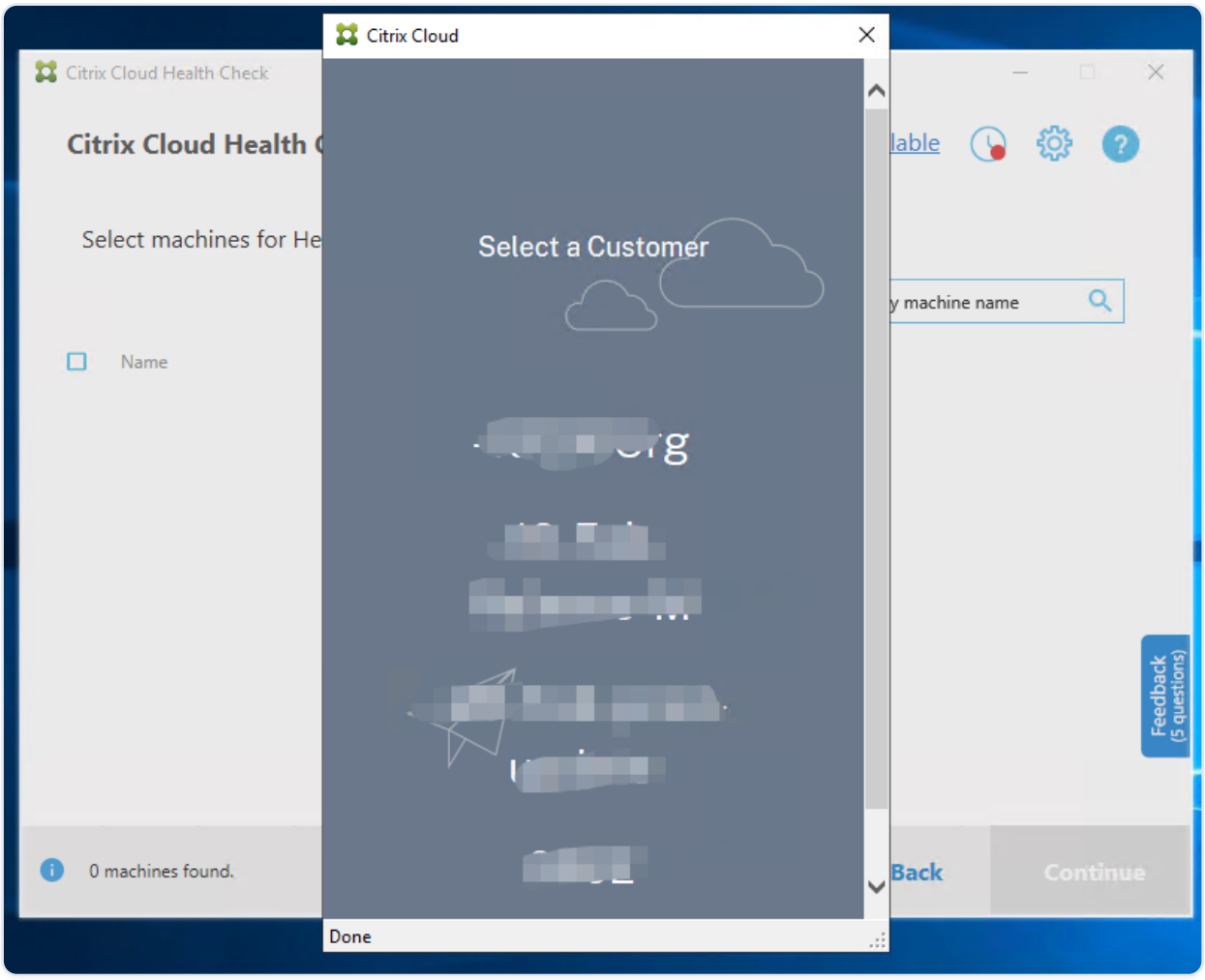
1. Prepare a new machine that is joined to the same domain forest as the machine Cloud Health Check runs on.
2. Open Cloud Health Check and click **Find machine** to sign in to Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



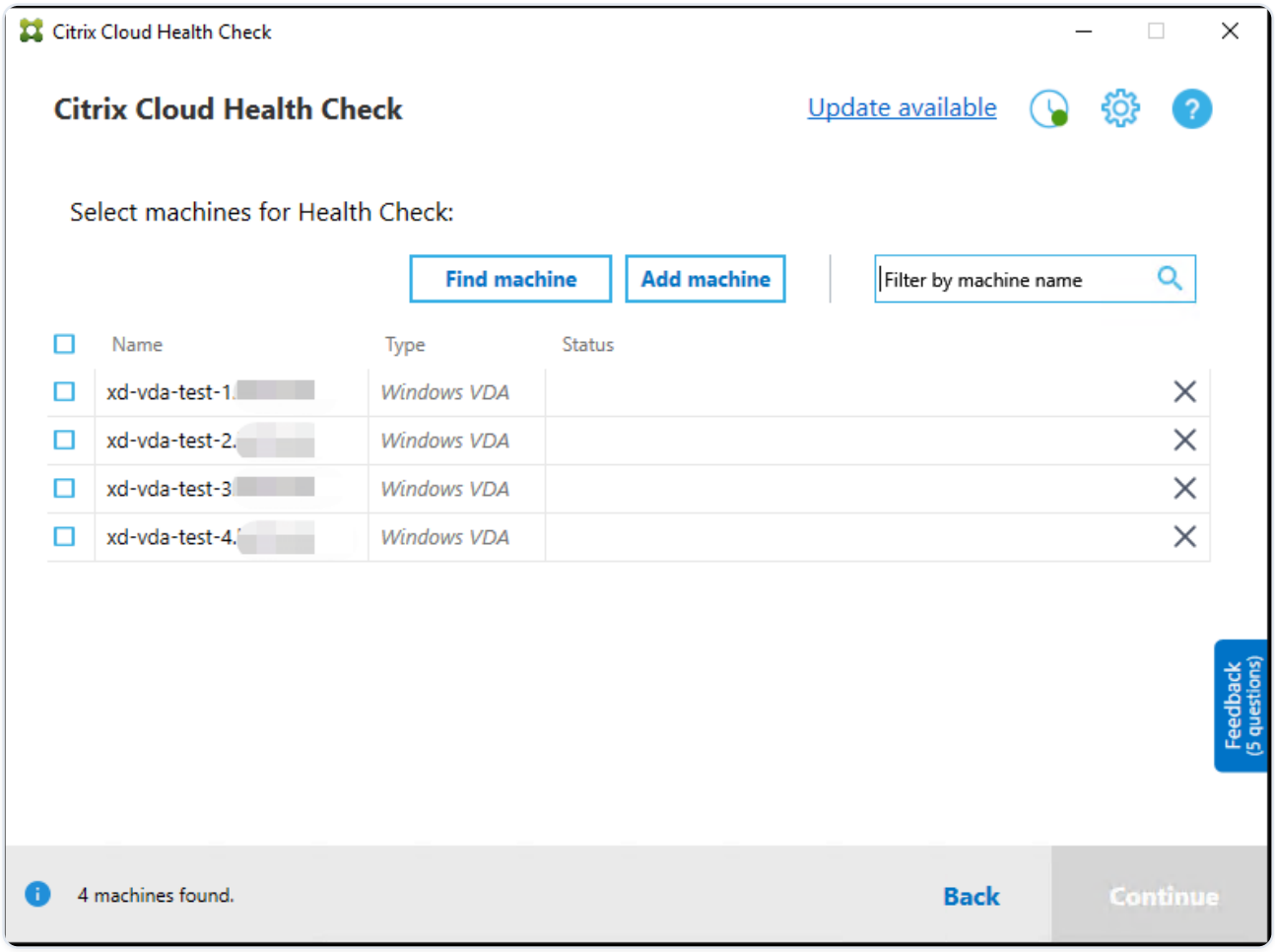
3. Select the customer with the cloud site you want to retrieve.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The VDA list displays in Cloud Health Check. The list is also saved in a local file located at `\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.json`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

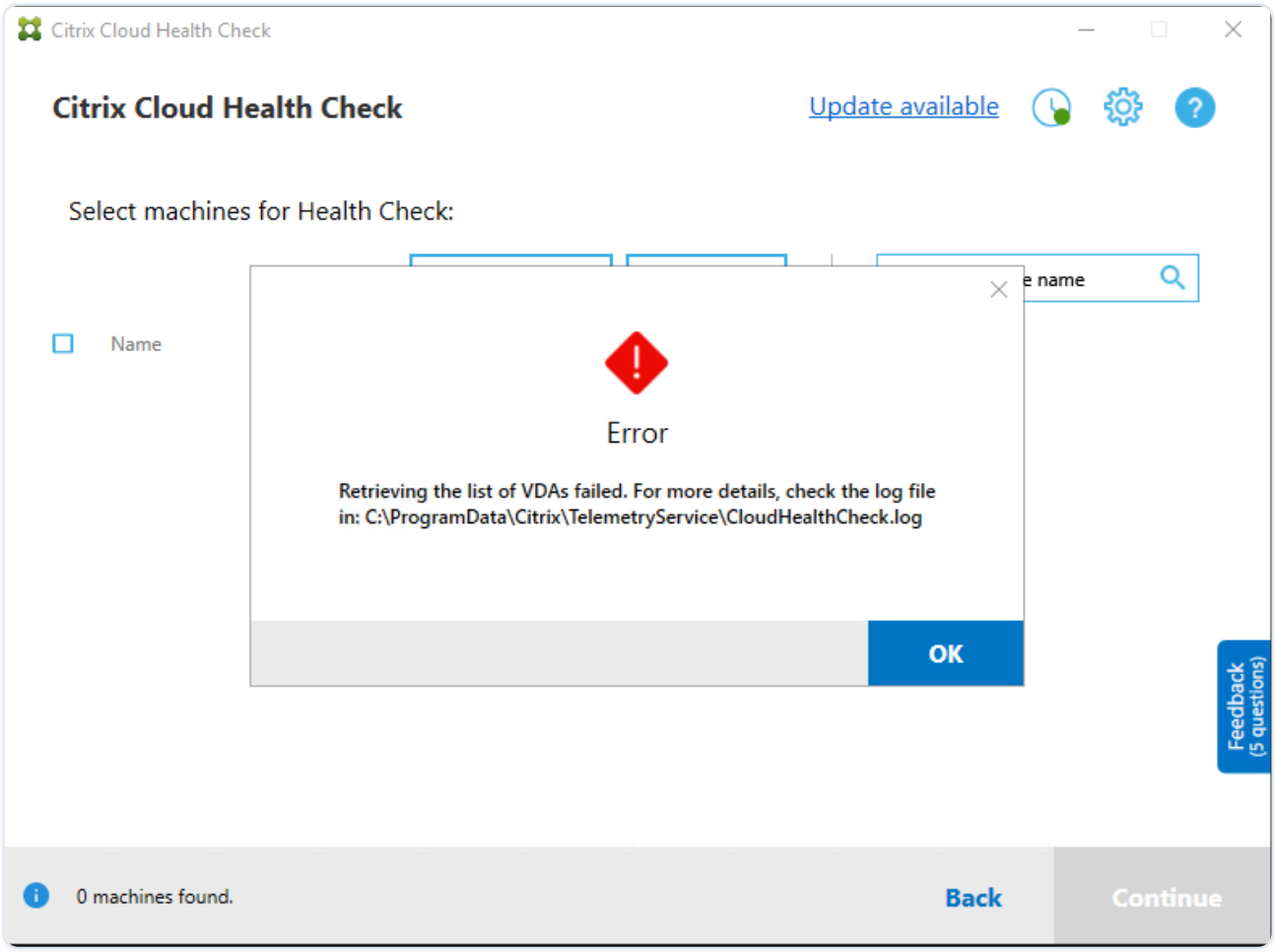


Your machine list loads the local cache when you open Cloud Health Check again. If you have made any updates in your deployment, you must click **Find machine** to refresh the machine list.

NOTE:

- Cloud Health Check finds machines only in the same domain forest as the machine Cloud Health Check runs on.
- Citrix Cloud sessions expire in one hour. After one hour, you must click **Find machine** again to get the latest VDA list.
- An error message pops up if retrieving the VDA list fails. You can check the details in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Heath check results

Health checks that generate reports contain the following elements:

- Time and date when the results report was generated
- FQDNs of the machines that were checked
- Conditions checked on the target machines

Running Cloud Health Check on the command line

Cloud Health Check can be run on the command line to help customers to perform health checks. To use Cloud Health Check on the command line, you must be an administrator on the machine Cloud Health Check is running on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

When using Cloud Health Check on the command line, only one machine can be checked at a time. Only one instance of `CloudHealthCheck.exe` can be run at the same time on the target machine. If you want to check multiple machines, the machines must be checked one by one, by wrapping the cmdlets in a loop in cmdlet/PowerShell scripts. Any opened UI instance of Cloud Health Check must also be closed.

Command-line arguments

The supported command-line arguments are:

- `MachineFQDN` - This argument is **mandatory**. This is the fully qualified domain name of the target machine.
- `MachineType` - This argument is optional. The argument value can be the Windows VDA (default value) or StoreFront.
- `ReportName` - This argument is optional. The argument value must be a valid file name on Windows. The default value is `HealthCheckReport`.
- `SkipAdminCheck` - This argument is optional. This can be added to skip the checks that require administrator permissions.
- `UpdateScripts` - This argument is optional. This can be added to update the check scripts from CDN server.
- `DisableCeip` - This argument is optional if CEIP is enabled on the UI, add it to disable CEIP.
- `Help` - Show help information about parameters.

Examples:

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -ReportName checkreport
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -SkipAdminCheck
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -UpdateScripts
```

```
HealthCheckCLI.exe -MachineFQDN
machine1.domain.local,machine2.domain.local,machine3.domain.local
```

```
HealthCheckCLI.exe -Help
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Parameter names are not case sensitive.

By default, the console output is not shown in the command line console window. You can manually display the output by appending `|more` to the argument.

Example: `HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

The command line default needs administrator permissions to run. Add the parameter `-SkipAdminCheck` to override the need for administrator permissions.

Exit codes

Exit codes explain the result of Cloud Health Check checks within the command line. To get the exit code, you must add `start /wait` before the command line.

Example: `start /wait HealthCheckCLI.exe -MachineFQDN machine.domain.local`

Exit codes are:

- 0 - Normal, check completed and passed.
- 1 - Failure, check completed with issues.
- 2 - Error, check not completed with errors.

You can also use the argument `echo %errorlevel%` to get the exit code for the last ran command.

Reports

Cloud Health Check creates folders with the name of the machine in `HealthCheckDataFolder` for the target machine. An .html file and a .json file are created on the machine Cloud Health Check is installed on. Health check reports are located in the `HealthCheckDataFolder` in `%ProgramData%\Citrix\TelemetryService\HealthCheck\Data`.

Reports are only created when issues exist on the target machine.

NOTE:

The report files are overwritten if the specified report name exists.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alerts and basic information are stored in the .json report.



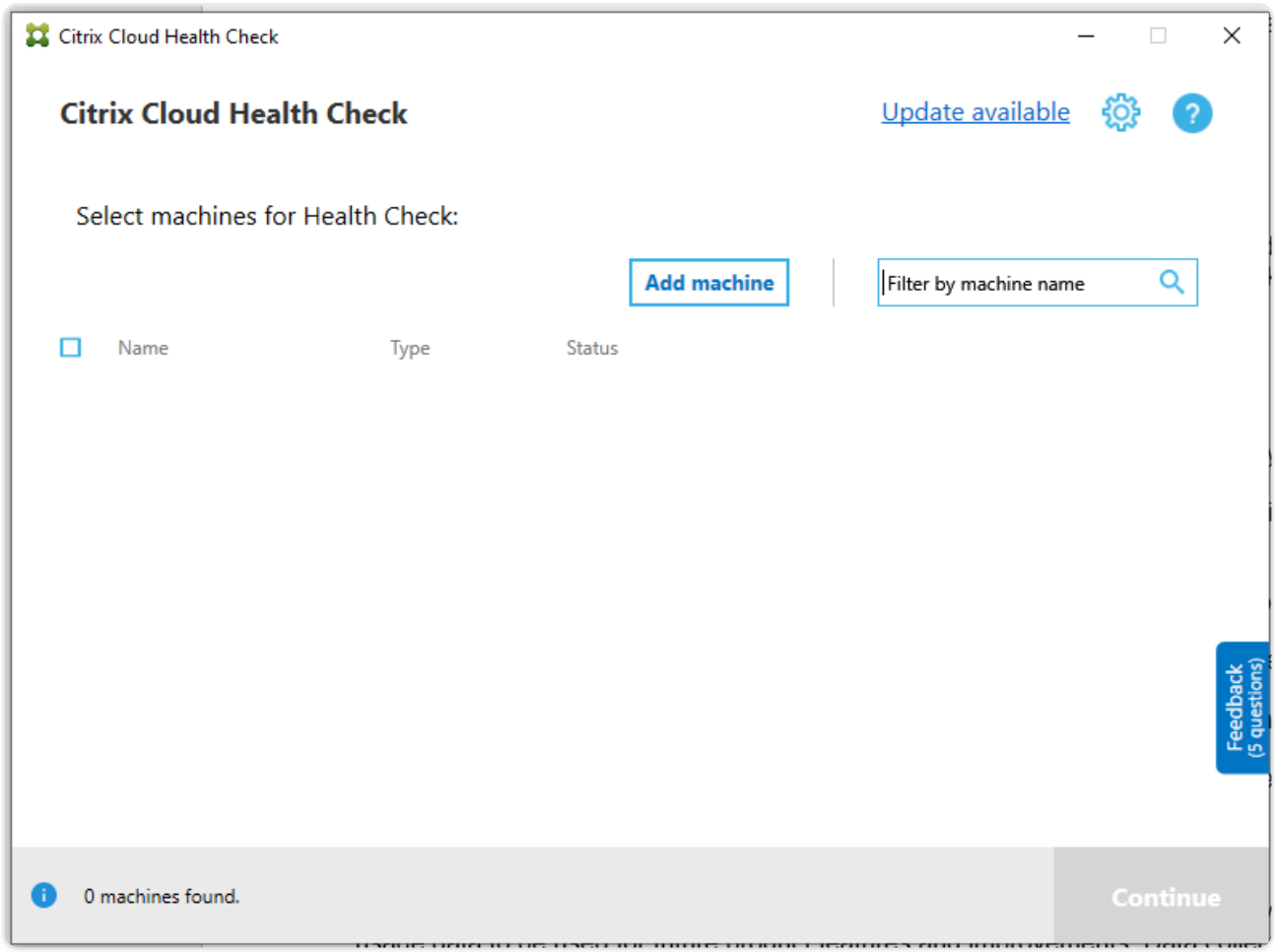
Report codes are:

- **issueKey**: a plain text description of the issue.
- **issueUuid**: a unique identifying string for the issue.
- **fixRecommendation**: the fix recommendation for the issue.
- **severity**: indicates if the issue must be fixed. An error can indicate that the component (VDA or StoreFront) malfunctioned, and a warning indicates that the component can work but might have some potential issues.
- **issueName**: the title of the issue.
- **issueDescription**: a detailed description of the issue.

Updating Cloud Health Check

If there is a new version of Cloud Health Check available, an Update available link displays on the top right of the Cloud Health Check window. Click the link to go to Citrix Downloads to get the new version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



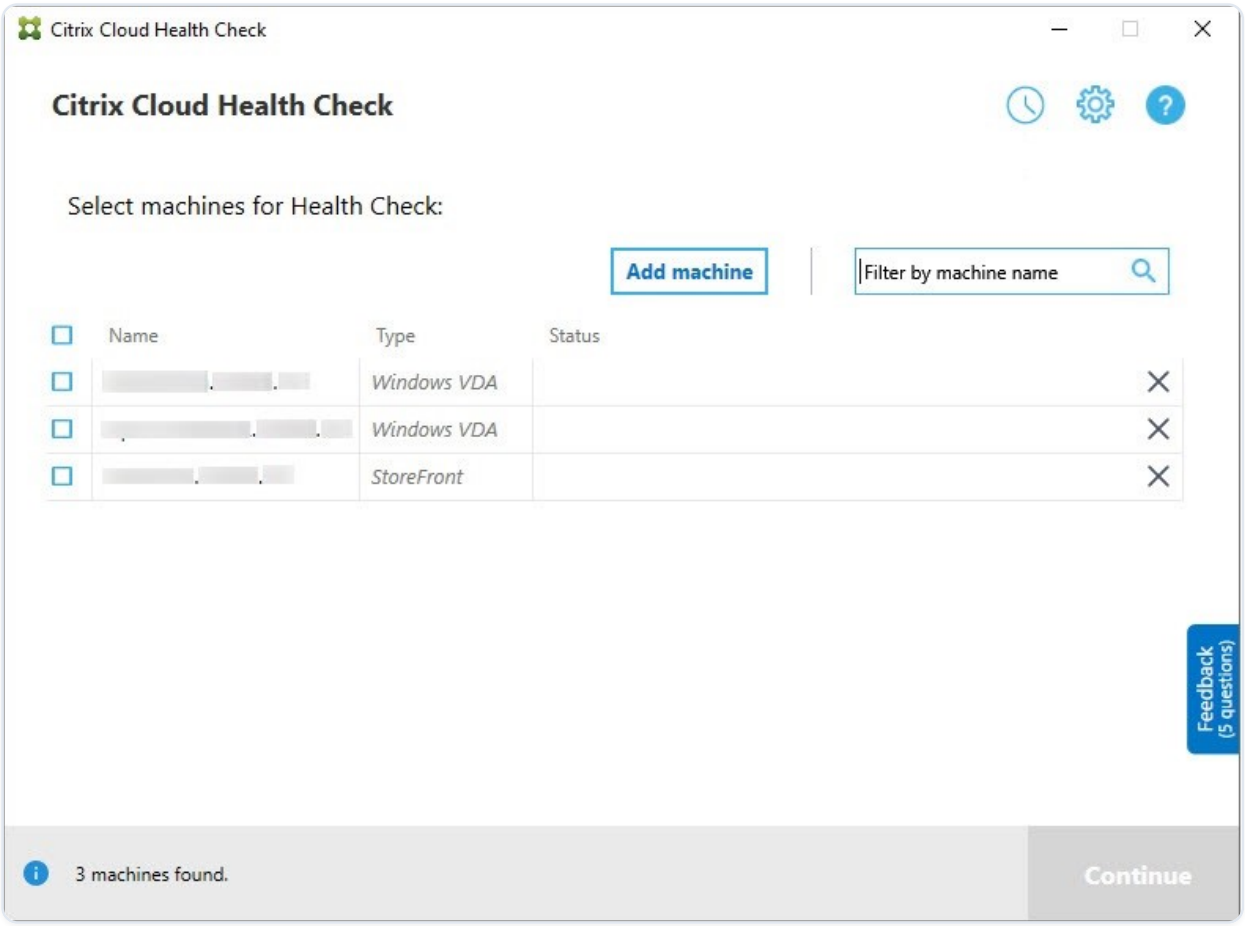
Cloud Health Check scheduler

Use the Cloud Health Check scheduler to perform periodic health checks.

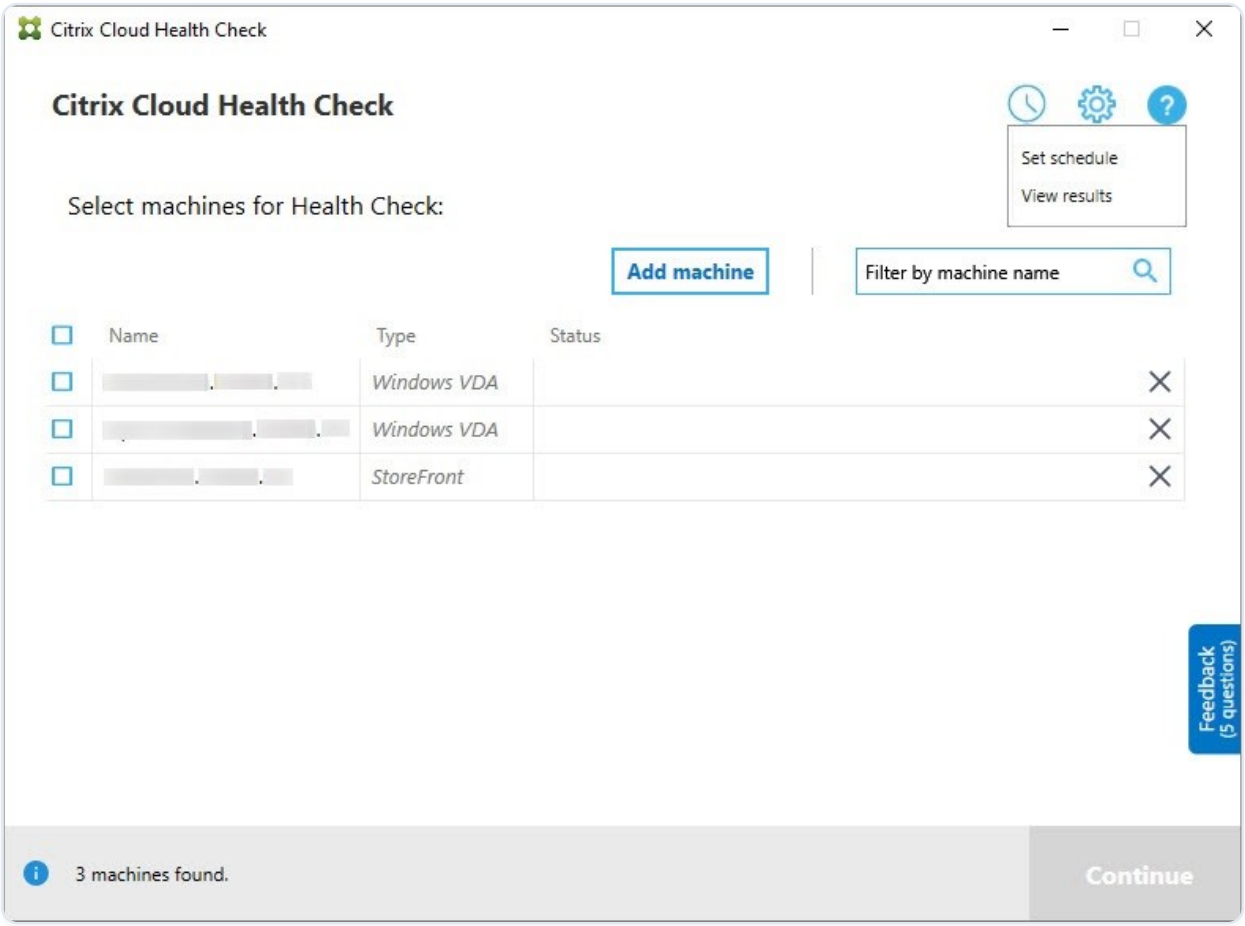
Set up the schedule

1. Click **Add machine** in the Cloud Health Check main window to add machines that you want to run periodic checks on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Click the clock icon, then click **Set schedule**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select a time for your schedule, then click **Next**. The task can be set to repeat by selecting the **Repeat task every** check box.
4. Choose to output results to Windows Event Log. The task can be set to write the results to Windows Event Log.
5. Choose to trigger a custom PowerShell script after the scheduled check finishes, and then click **Next**.

    - Click **Edit** to edit the script content in Windows PowerShell ISE if needed.
    - Click **Locate** to open the file location and to use a different editor to open the file to edit the script.
    - Click **Reset** to reset the script to its original setting.

    NOTE:

    - You cannot change the script name and path for the script.
    - You can implement custom actions using the ChcShceduledTrigger.ps1 script, such as sending an email after the scheduled check report is ready. Add the following code to the end of the script. Customize the code to add the correct email accounts and the SMTP server address. An email notification is sent using the credentials of the account that the scheduled task runs.

```
#Sending email example code:

$body = "CreatedTime: $($report.CreatedTime)"

$body = $body + "`nStatusCode: $($report.StatusCode)"

$body = $body + "`nMachineCount: $($report.MachineReports.Count)"

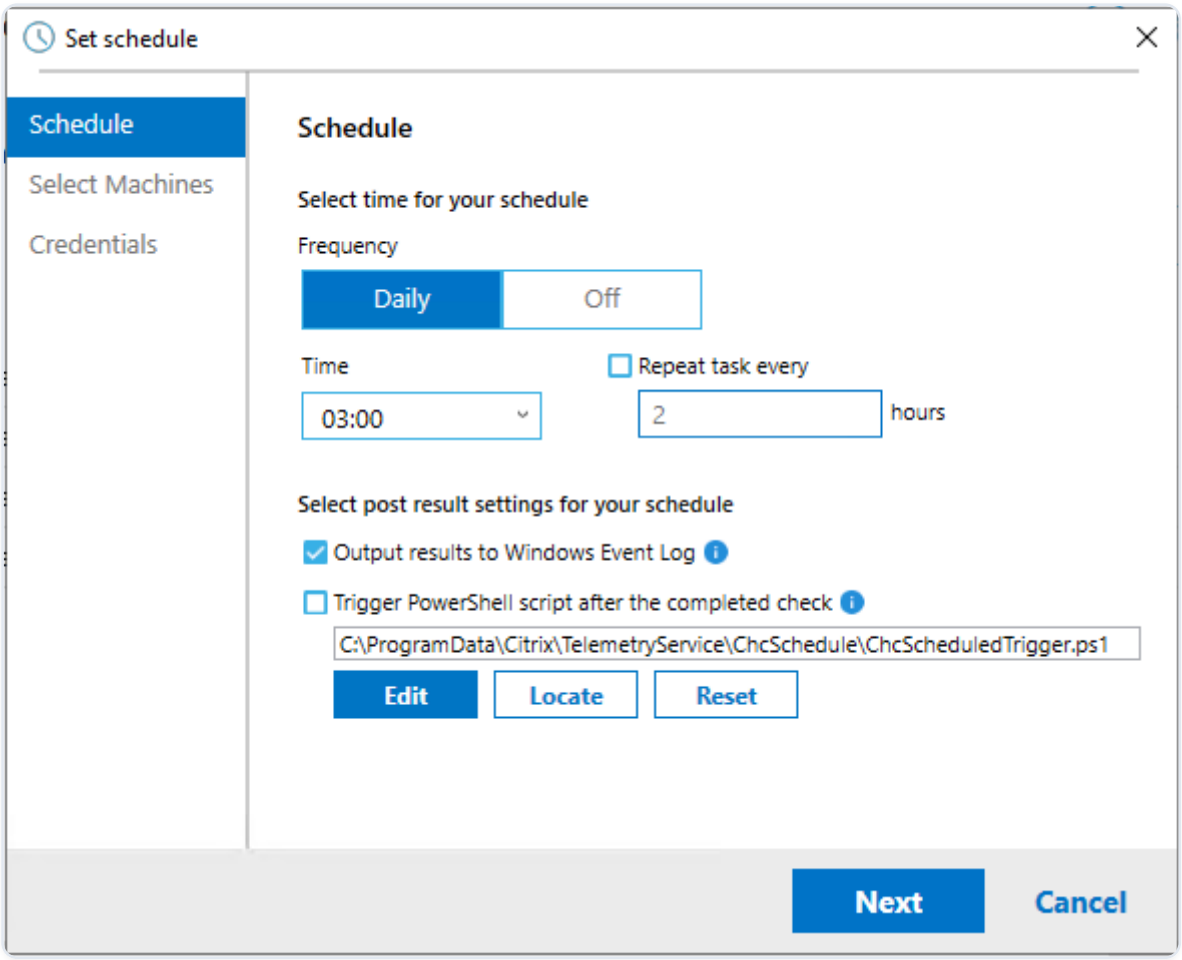
$from = "mock_email_accout"

$to = "mock_email_accout"

$smtpServer = "mock_smtp_server"
```

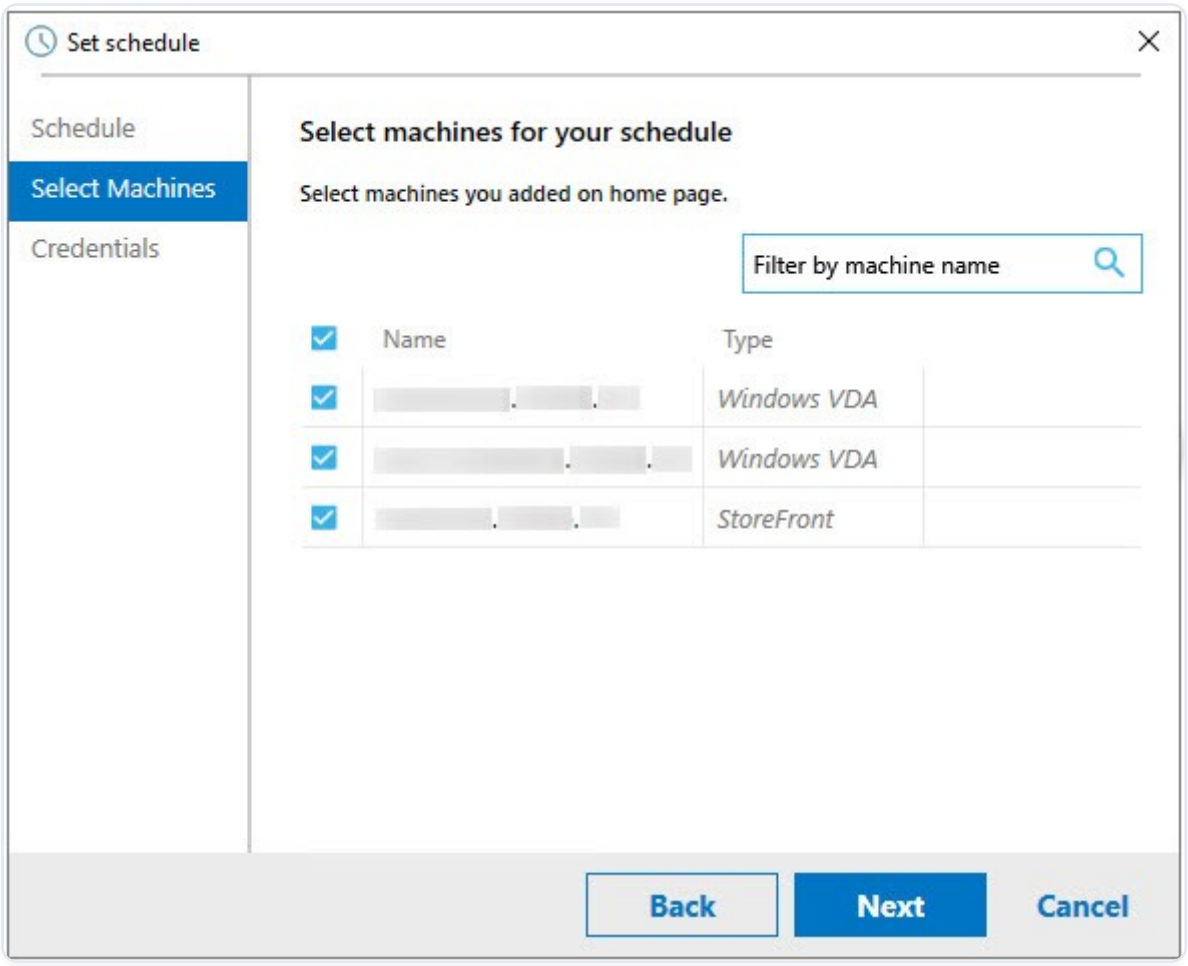
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler Report"
-Body $body -From $from -To $to -SmtpServer $smtpServer
```



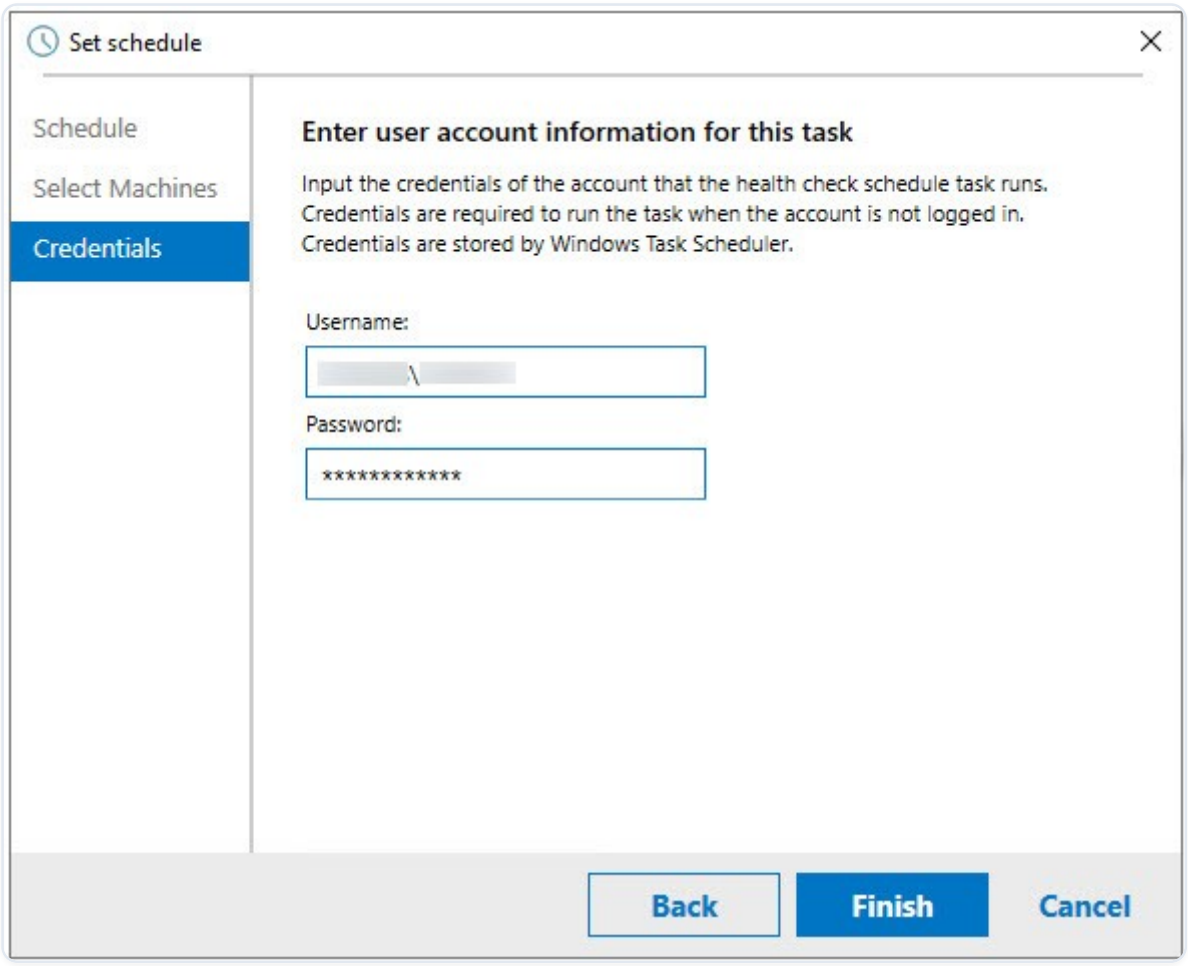
6. Select the machines for your schedule, then click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

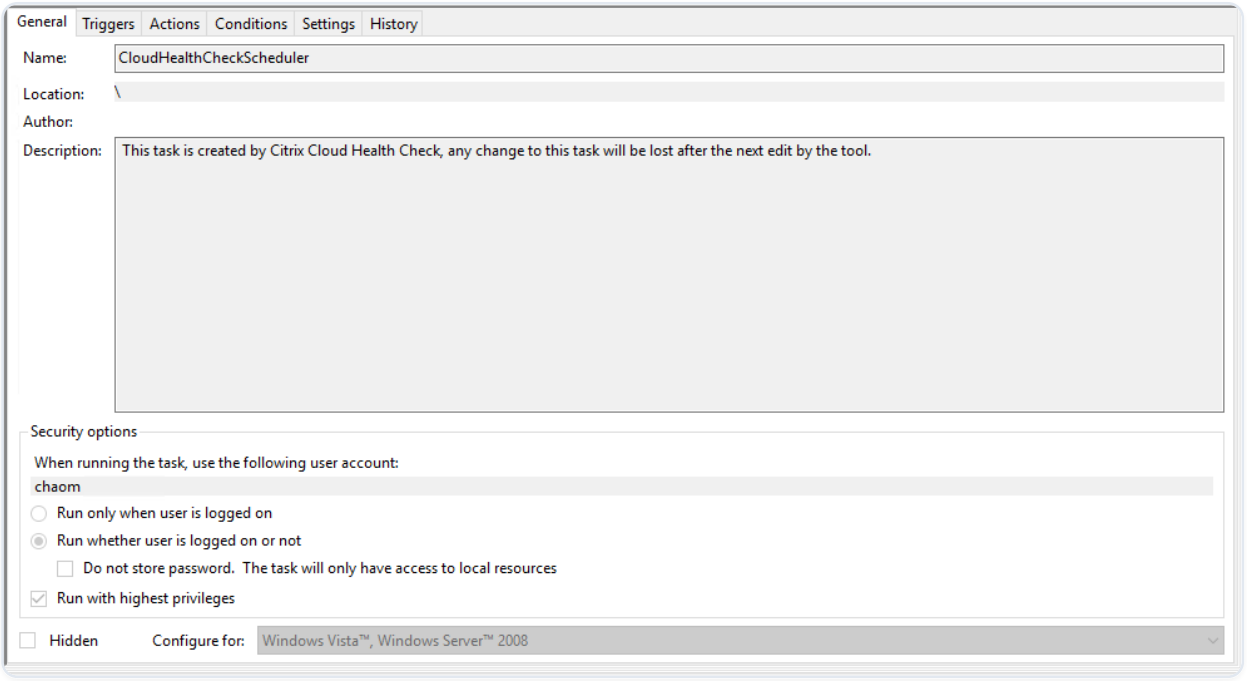


7. Input the credentials of the account that the task runs on, then click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



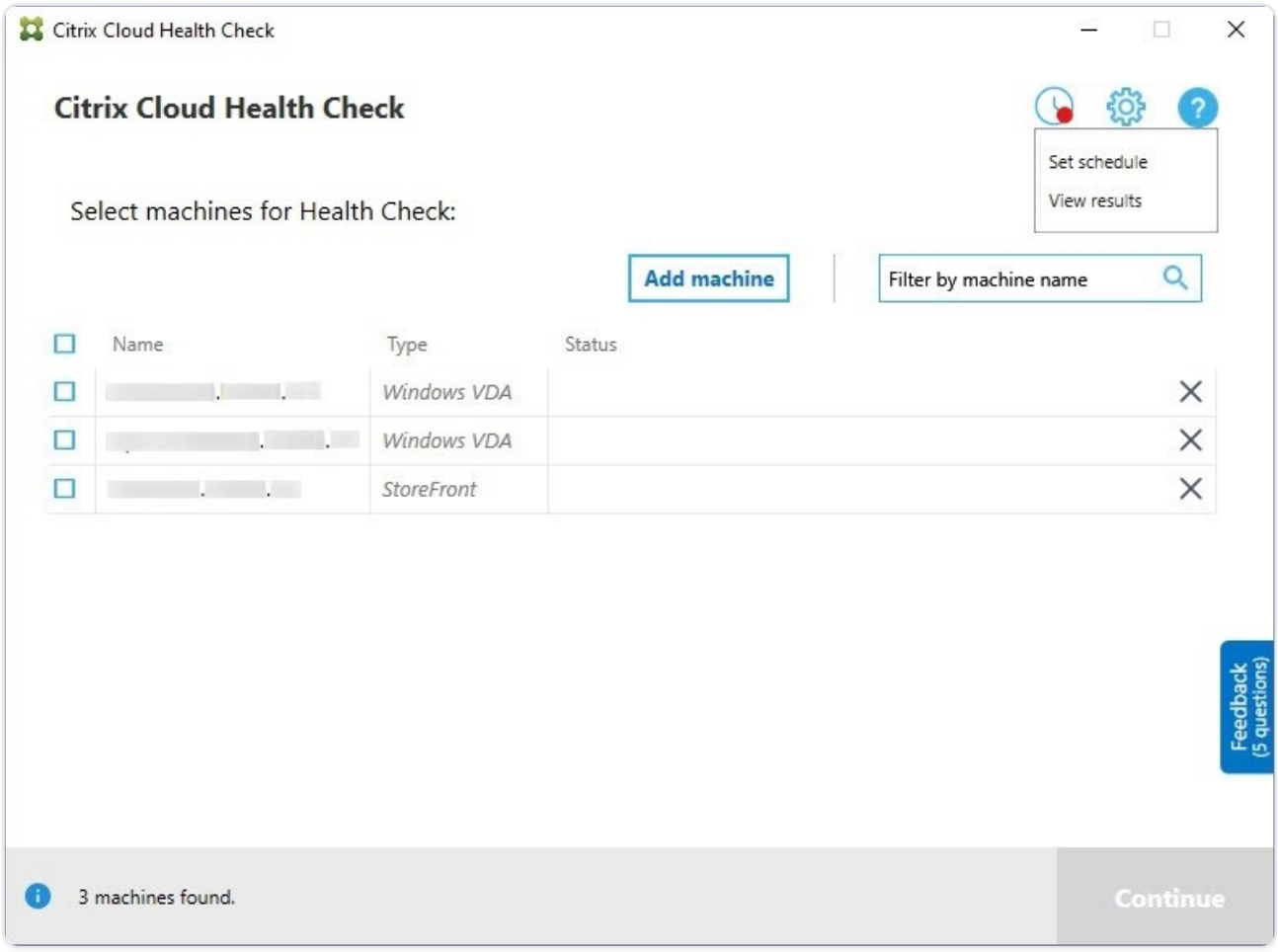
8. A CloudHealthCheckScheduler task is created in Windows Task Scheduler.



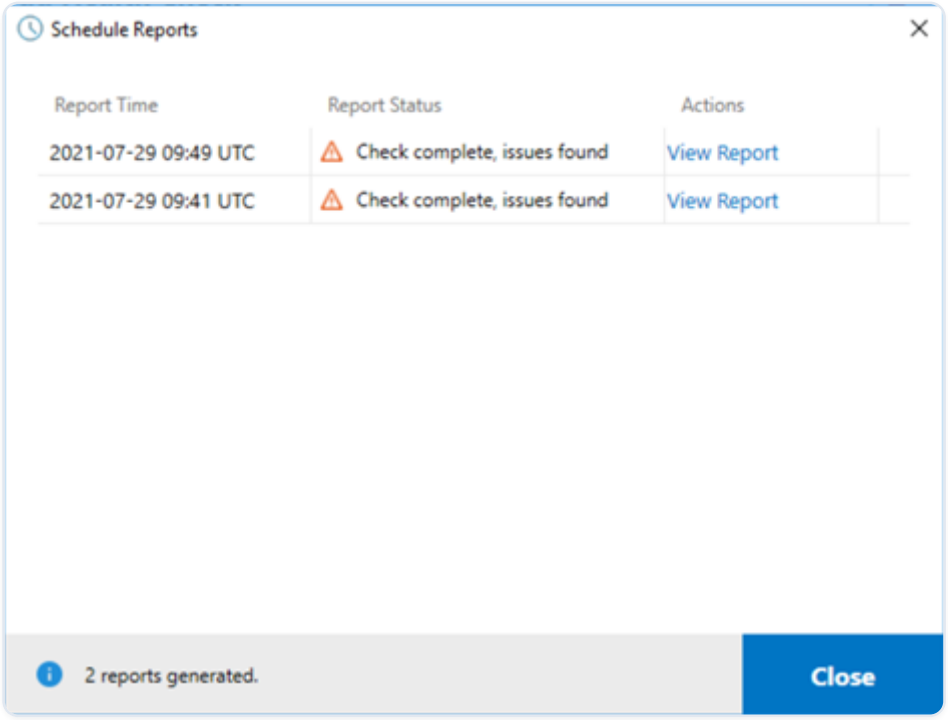
View schedule results

The clock icon with a red dot indicates that issues were found in the last check. To view the results, click the clock icon, then click **View results**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

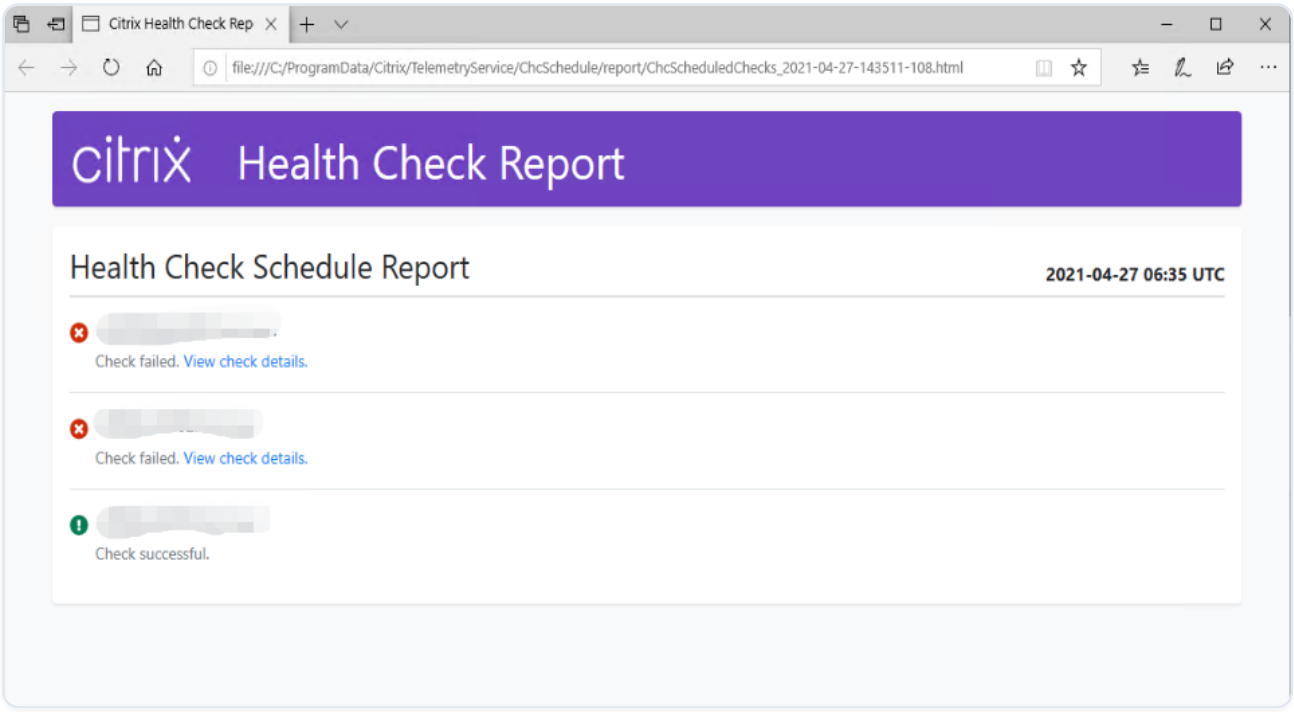


The Schedule Reports page shows the results for all the scheduled health check tasks. Click **View Report** to check the report for each schedule.

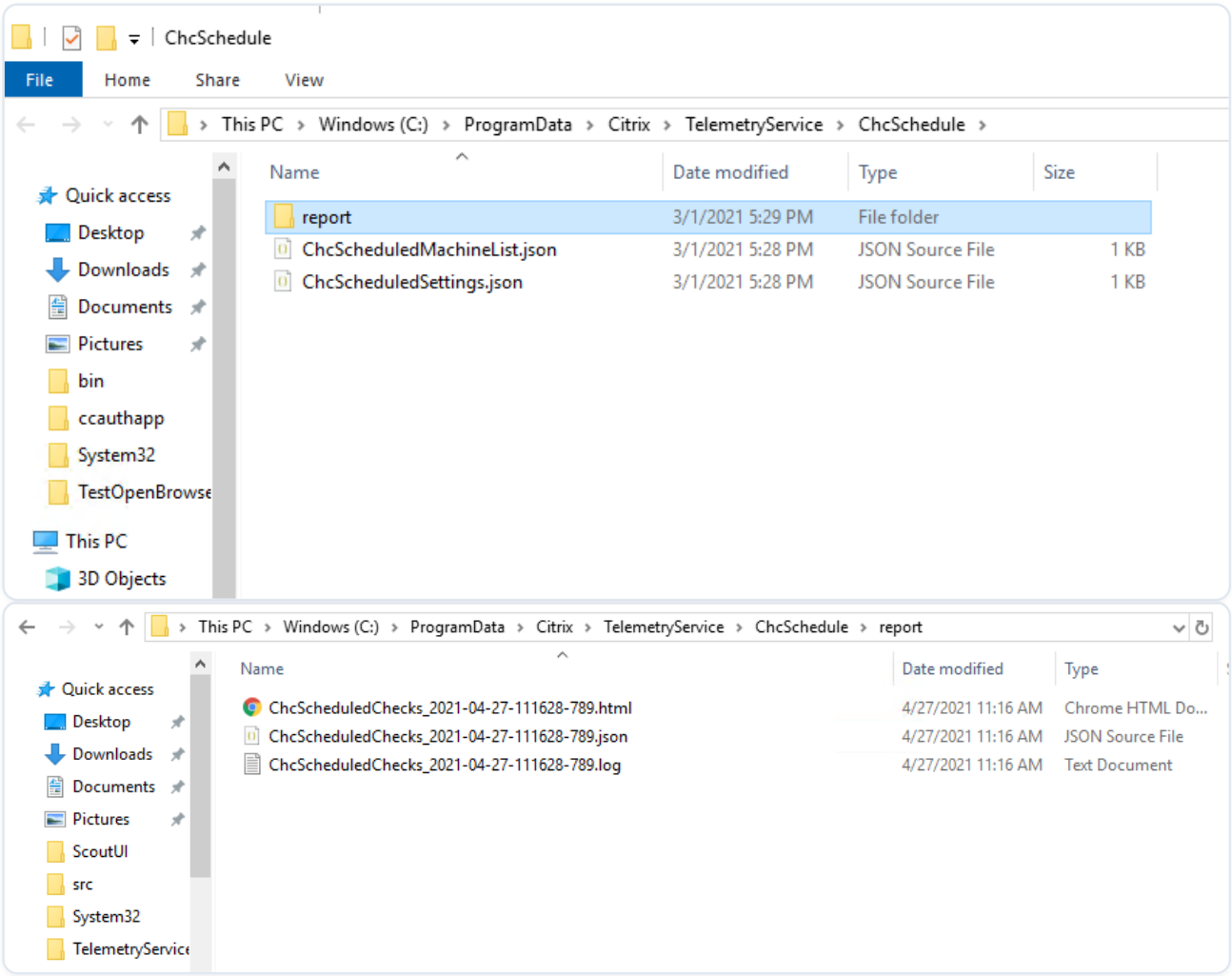


The html report lists the overall report for each schedules. An example of the report is below:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

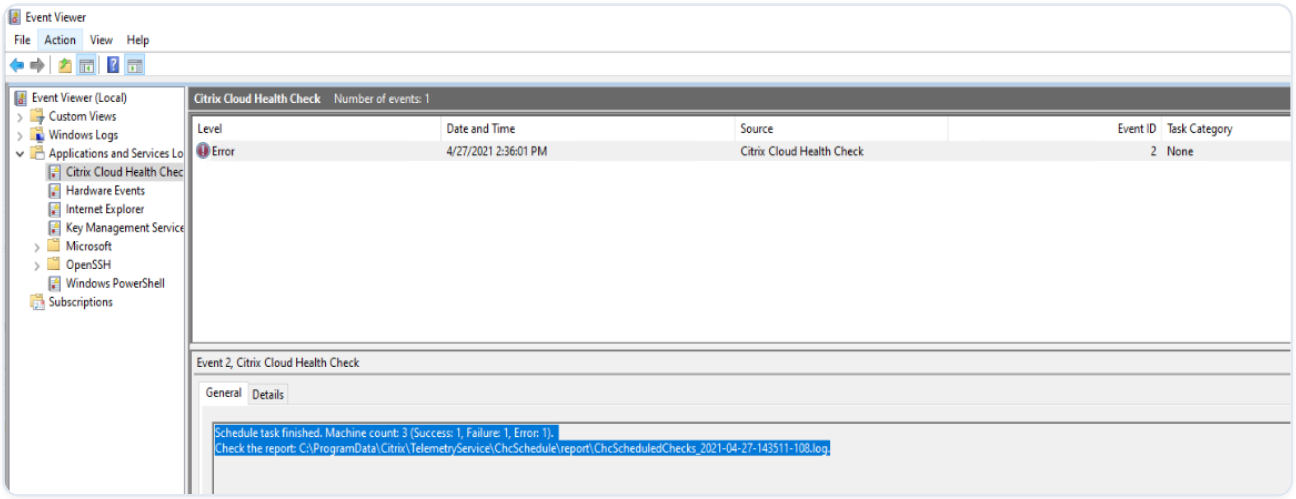


All health check results are stored in a folder called ChcSchedule. Cloud Health Check creates three files during each check run. Up to 500 iteration logs are kept.



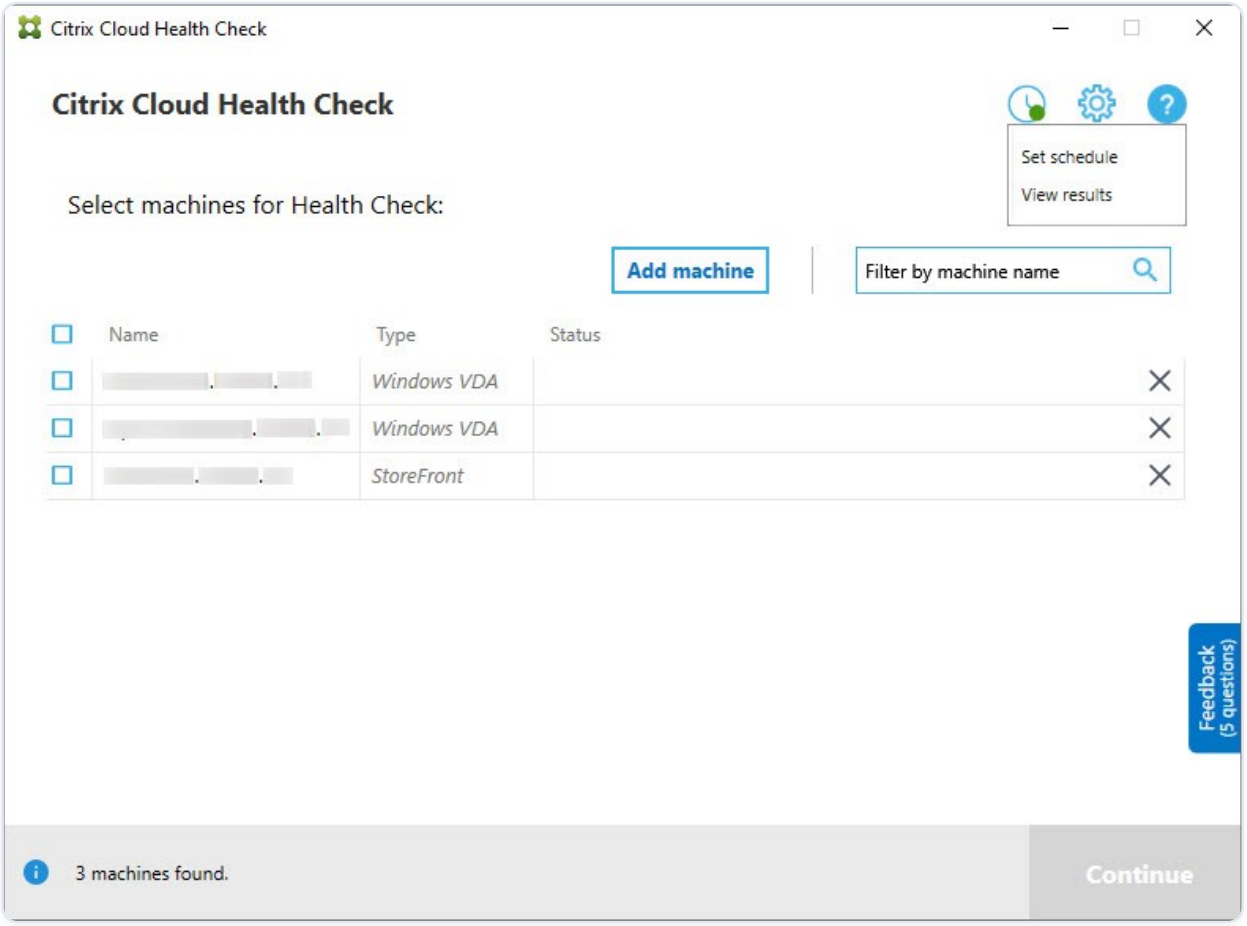
© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the **Output results to Windows Event Log** checkbox is selected, the check result is also sent to Window Event Log.



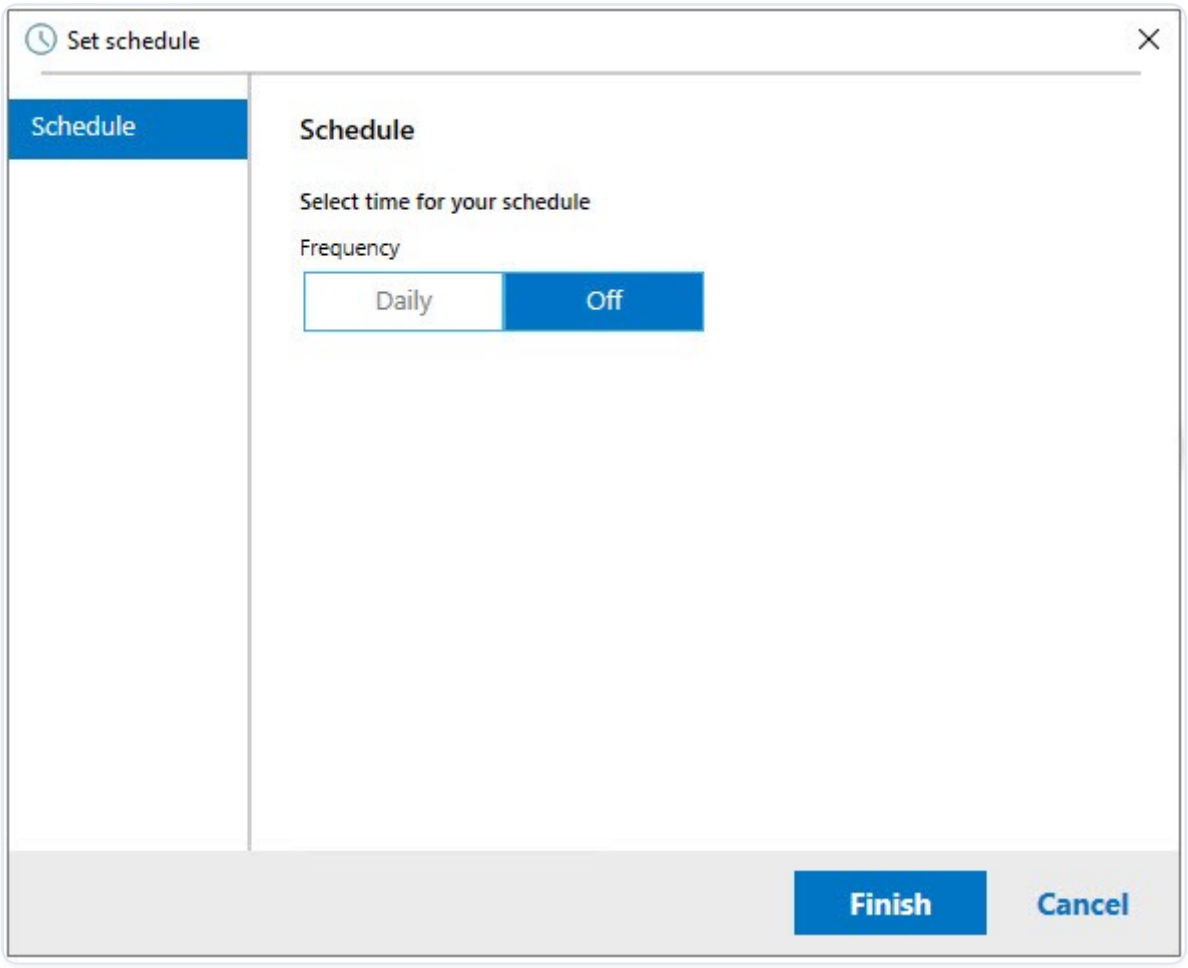
Disable schedules

1. Click the clock icon, then click **Set schedule**.



2. Click **Off**, then click **Finish** to disable the scheduler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



More information

- You must add or import VDAs to Cloud Health Check first. For more information, see Import VDA Machines.
- The Cloud Health Check scheduler can only schedule one task at a time on a domain-joined machine. If you set the schedule multiple times, only the latest one takes effect.

Verification tests

Before a health check starts, verification tests run automatically for each selected machine. These tests make sure that the requirements are met for a health check to run. If a test fails for a machine, Cloud Health Check displays a message with suggested corrective actions.

- **Cloud Health Check cannot reach this machine** - Ensure that:
  - The machine is powered on.
  - The network connection is working properly. (This can include verifying that your firewall is properly configured.)
  - File and printer sharing is turned on. See the Microsoft documentation for instructions.

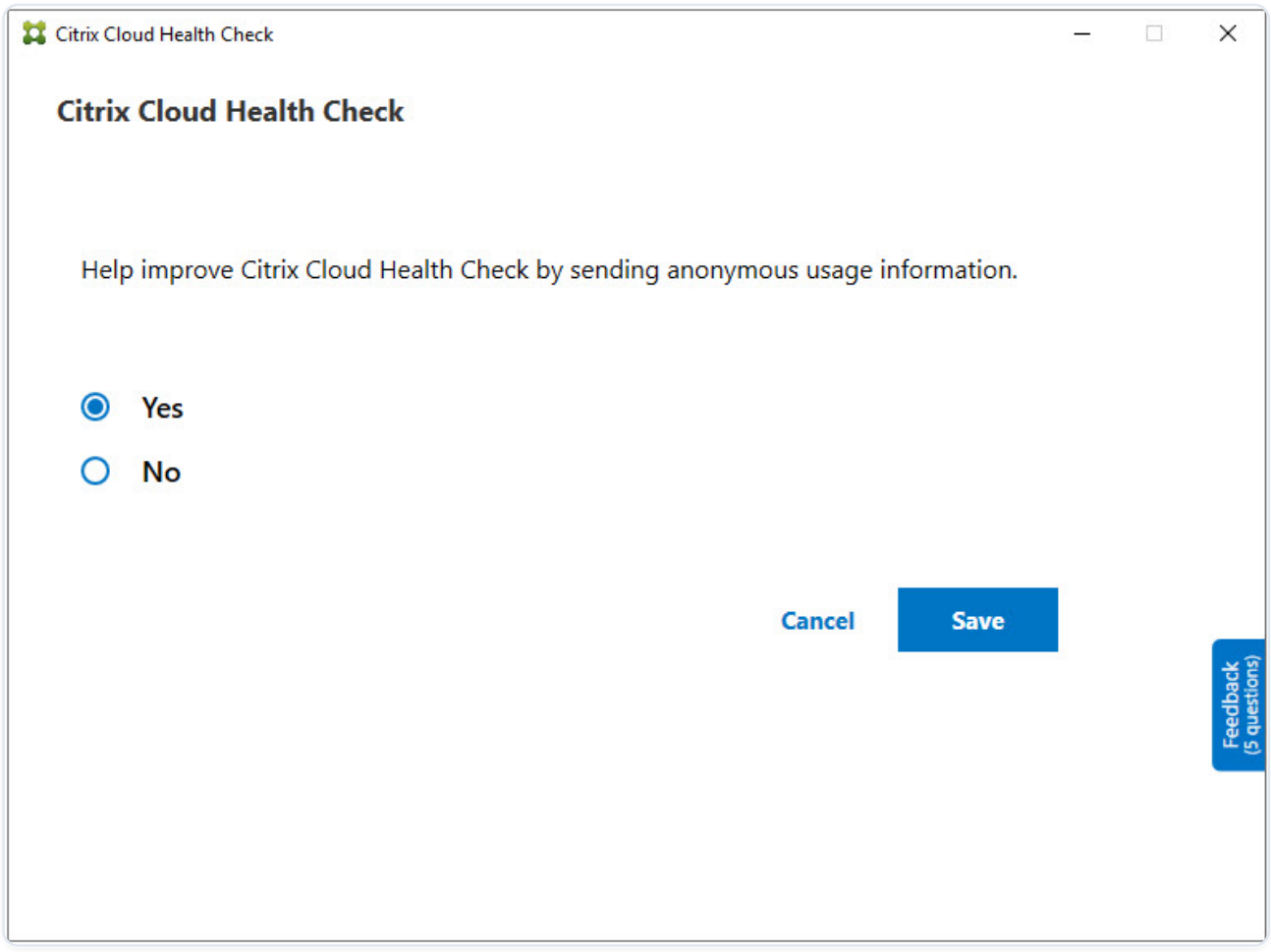
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Enable PSRemoting and WinRM** - You can enable PowerShell remoting and WinRM by running PowerShell as an administrator, then running the Enable-PSRemoting cmdlet. For details, see the Microsoft help for the cmdlet.
- **Cloud Health Check requires PowerShell 3.0 or later** - Install PowerShell 3.0 or later on the machine, and then enable PowerShell remoting.
- **WMI is not running on the machine** - Ensure that Windows Management Instrumentation (WMI) access is enabled.
- **WMI connections blocked** - Enable WMI in the Windows Firewall service.

Usage data collection

When you use Cloud Health Check, Citrix uses Google Analytics to collect anonymous usage data to be used for future product features and improvements. Data collection is enabled by default.

To change usage data collection and upload, click the **Settings** gear in the Cloud Health Check UI. You can then choose whether to send the information by selecting **Yes** or **No** and then clicking **Save**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Automatic fix

Automatic fix allows Cloud Health Check to automatically detect and fix certain issues by changing the settings or restarting the services.

Automatic fix checks the following VDA registration items, with the recommended fixes:

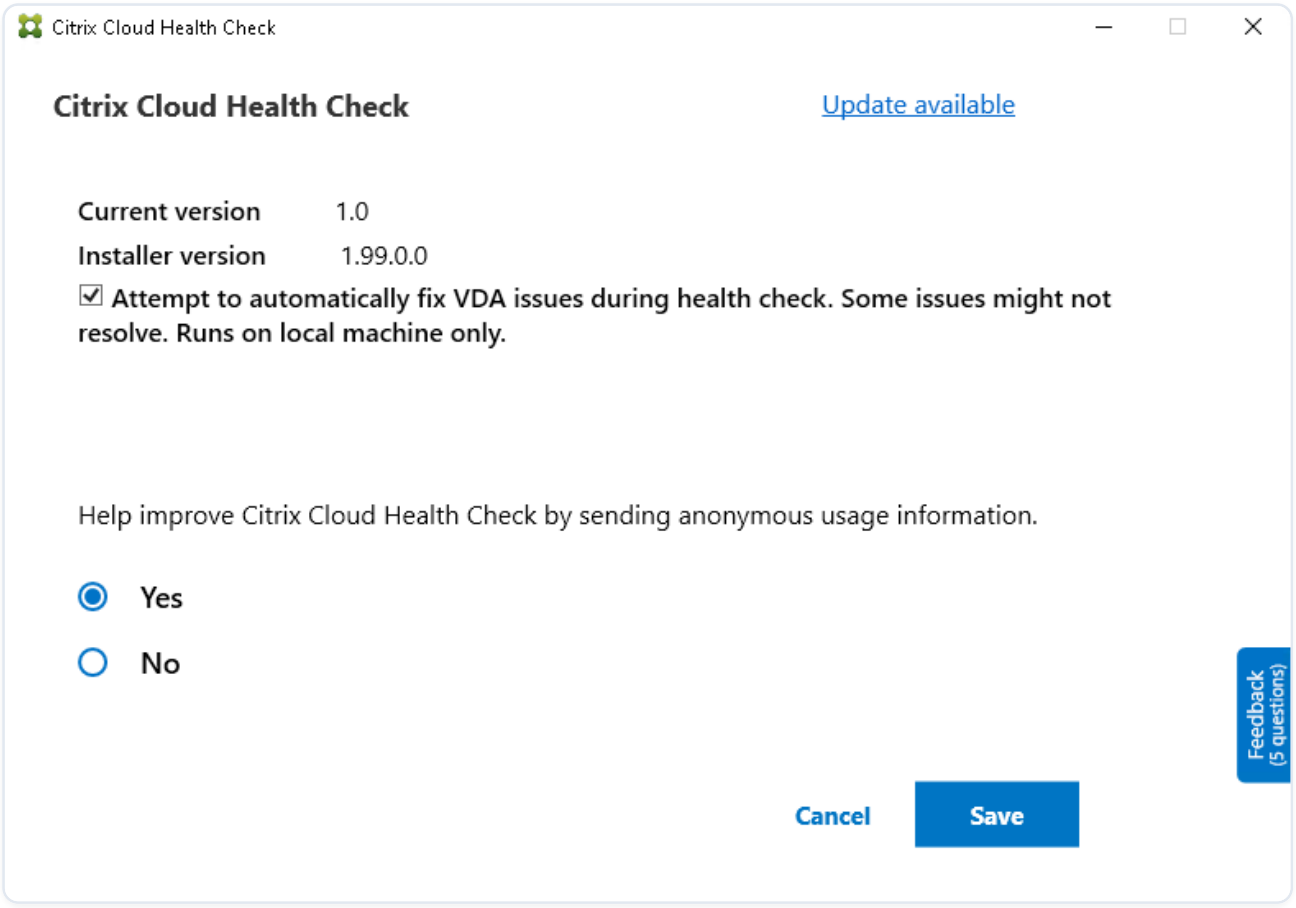
- VDA machine domain membership
  - Fix: Test connection security channel with a "repair" model to fix
- VDA services status
  - Fix: Restart BrokerAgent service
- Communication with Controller
  - Fix: Restart BrokerAgent service
- Time sync with Controller
  - Fix: Run W32tm command

For session launches, automatic fix checks the following item, with the recommended fix:

- Session launch service status
  - Fix: Restart BrokerAgent service

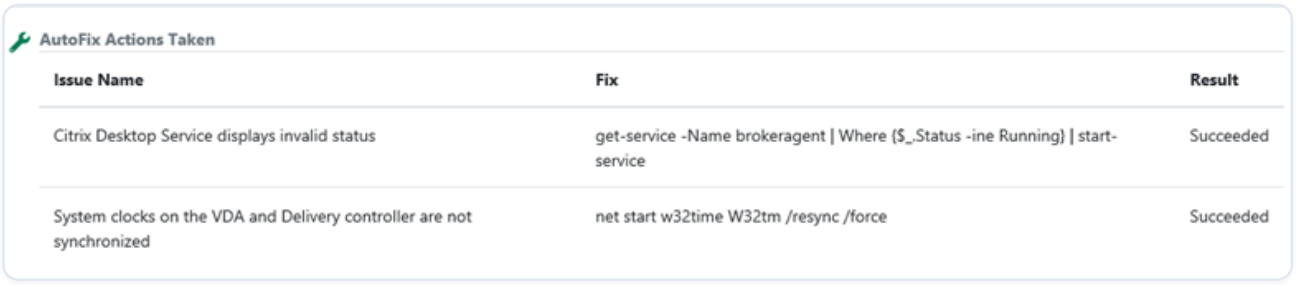
This feature is enabled by default. To disable it, click the gear icon in the upper right corner of the Cloud Health Check main window and then clear **Attempt to automatically fix VDA issues during health check**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

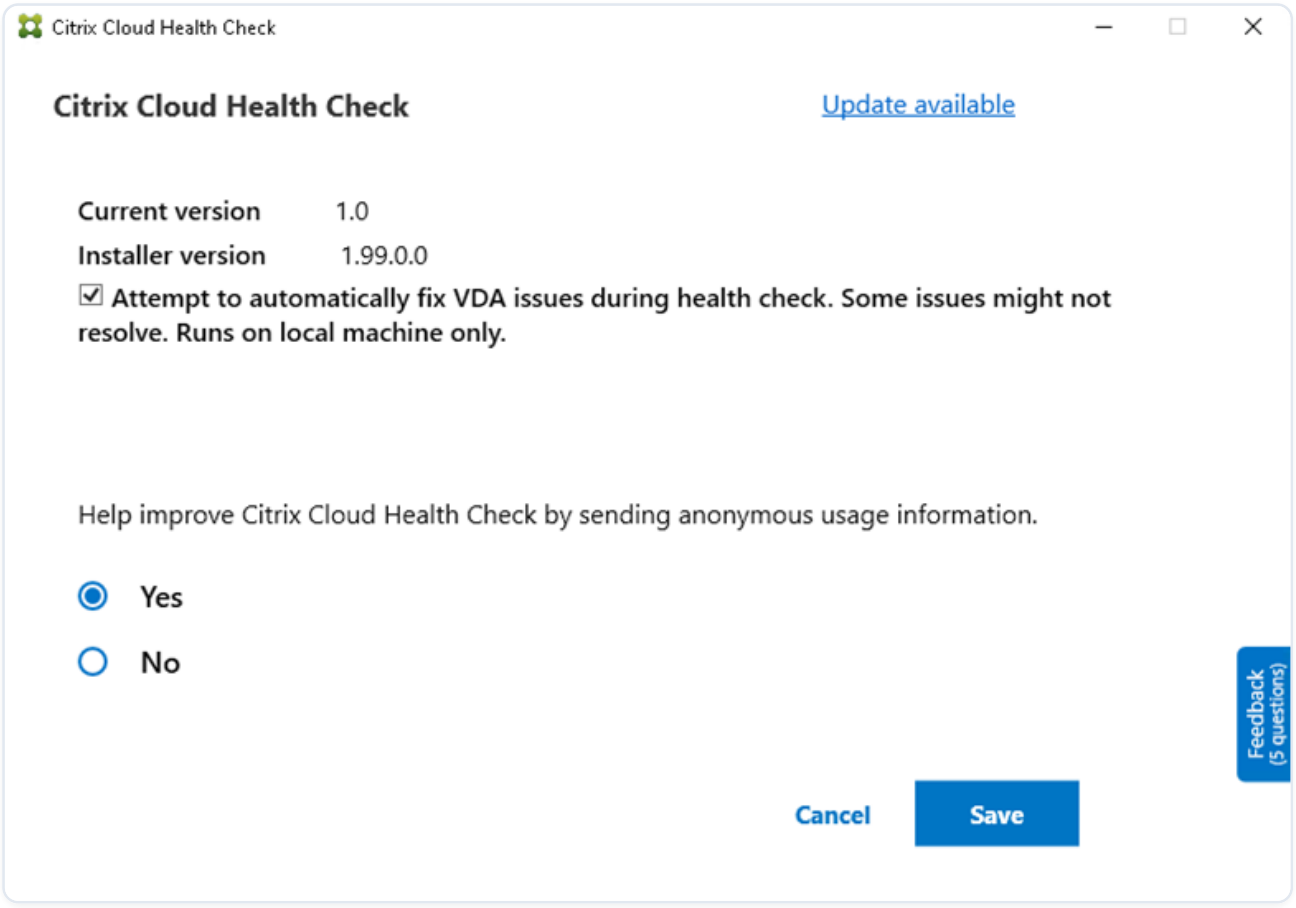


Result report

After running automatic fix, there is a section in the check results report to show all the details:



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Troubleshooting

When Cloud Health Check fails to run or any exception occurs, check the Cloud Health Check log in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.

The Cloud Health Check log for each target machine is in `C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\$TargetMachineFQDN\log.txt`.

To enable the debug log:

Edit `C:\Program Files\Citrix\CloudHealthCheck\CloudHealthCheck.exe.config`, update `<add name="TraceLevelSwitch" value="3" /> to <add name="TraceLevelSwitch" value="4" />`, save the file and reopen Cloud Health Check.

Feedback

To leave feedback on Cloud Health Check, fill out the Citrix survey.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration logging

NOTE:

Configuration log records appear only in English, regardless of which language you select for your Citrix Cloud account. Dates and times associated with those records are in MM/DD/YY format, expressed in Coordinated Universal Time (UTC).

Configuration logging is a feature which captures Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployment configuration changes and administrative activities to a logging database in Citrix Cloud. You can use the logged content to:

- Diagnose and troubleshoot problems after configuration changes are made. The log provides a breadcrumb trail.
- Assist change management and track configurations.
- Report administrative activities.

In this Citrix DaaS™, configuration logging is always enabled. You cannot disable it.

From Studio, you can view configuration log content, filtered by date ranges or by full text search. You can also generate a CSV report using PowerShell. From this console, you cannot edit or delete log content. You can use the Remote PowerShell SDK to schedule periodic data deletion from the log.

Update the retention of DaaS configuration logs

To maintain the performance of DaaS tenants, starting September 9th, 2024 configuration log retention will be set to 180 days.

Logs older than 180 days on September 9th, 2024 will be deleted. As we keep growing our DaaS Limits for a single DaaS tenant, this implementation ensures the best performance and resilience for our customers.

As a best practice, we advise customers to have a quarterly export mechanism. This can be done through PowerShell, see Generate reports. We also recommend customers schedule periodic date deletion, see Schedule periodic data deletion.

Permissions required (see Delegated administration):

- Full Administrators in Citrix Cloud™, plus Citrix DaaS Cloud Administrators and Read Only Administrators can view configuration logs in Studio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Full Administrators and Cloud Administrators can also download a CSV report of logging activity, using PowerShell.

What is logged

The following operations are logged:

- Configuration changes and administrative activities initiated from the **Manage** section and **Monitor** node
- PowerShell scripts
- REST API requests

NOTE:

You cannot see log entries for Citrix Cloud platform internal operations, such as database setup and management.

Examples of logged configuration changes include working with (creating, editing, deleting, assigning):

- Machine catalogs
- Delivery groups (including changing power management settings)
- Administrator roles and scopes
- Host resources and connections
- Citrix® policies through Studio

Examples of logged administrative changes include:

- Power management of a virtual machine or a user desktop
- Manage or monitor functions sending a message to a user

The following operations are not logged. (Many of them are not available to customer administrators.)

- Automatic operations such as pool management power-on of virtual machines.
- Policy actions implemented through the Group Policy Management Console (GPMC). Use Microsoft tools to view logs of those actions.
- Changes made through the registry or from sources other than Studio, Monitor, or PowerShell.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View configuration log content

To view configuration log content, follow these steps:

1. Sign in to Citrix Cloud.
2. In the **DaaS** tile, click **Manage**.
3. Select **Logging** in the left pane and click the **Events** tab.

By default, event logs are listed by administrator names. You can perform the following tasks as needed:

- **Sort the display.** Sort the display by clicking a column header.
- **Filter logs.** Refine the display by setting filters, such as:
  - Day intervals or custom periods.
  - Complete or partial Main Task names.
  - Low-level operation details, such as machine name and VDI name. To search across low-level details, select **Extend search scope to include details** before entering your search term.

    NOTE:

    - Enabling this option can increase the search time because the system searches a broader set of log entries.
    - The selection is saved only for the current Web Studio session. When you sign out or start a new session, select the option again if you want to include low-level operation details in the search.
- **Export logs.** Export selected or all logs to a CSV file for archiving or further analysis.
- **Customize columns.** Tailor the display to your needs by adding non-default columns such as Client IP and Labels.
- **Manage labels.** Add, edit, and remove labels for event logs to enhance log organization and tracking.

Display characteristics:

- High-level operations created during management and monitoring are listed in the upper middle pane. A high-level operation results in one or more services and PowerShell SDK calls, which

© 1997–2026 Citrix Systems, Inc. All rights reserved.

are low-level operations. When you select a high-level operation in the upper middle pane, the lower pane displays the low-level operations.

- If you create a low-level operation in PowerShell without specifying a parent high-level operation, configuration logging creates a surrogate high-level operation.
- If an operation fails before completion, the log operation might not be completed in the database. For example, a start record has no corresponding stop record. In such cases, the log indicates that there is missing information. When you display logs based on time ranges, incomplete logs are shown if the data in the logs matches the criteria. For example, if you request logs for the last five days, and a log with a start time in the last five days has no end time, it is included.
- Remember: You cannot see log entries for Citrix Cloud platform internal operations, such as database setup and management.

View tasks related to machine catalog operations

To view tasks related to machine catalog operations, navigate to **Logging > Tasks**. The **Tasks** tab displays only tasks related to catalogs created through Machine Creation Services™ (MCS) or Provisioning Services (PVS). Specifically, tasks associated with the following machine catalog operations appear:

- Create catalogs
- Clone catalogs
- Add machines
- Remove machines
- Update a catalog (update images or machines)
- Roll back machine updates

TIP:

The **Tasks** tab displays only tasks related to provisioning scheme changes (creating or modifying a provisioning scheme).

A task can be in the following state:

- Completed
- Not started

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Running
- Canceled
- Failed
- Unknown

To cancel a running task, select the task and then click **Cancel**. The cancelation takes some time to complete.

Examples of logged tasks include:

- Image update completed for a certain catalog
- Error while updating the image for a certain catalog
- Canceled image update for a certain catalog
- Provisioning VMs to a certain catalog
- Removing VMs from a certain catalog
- Created a certain catalog

By default, the display in the center pane lists logged tasks chronologically (newest entries first), separated by date. You can sort the display by column header. To clear completed tasks, click **Clear Completed Tasks** under the **Tasks** tab. To choose which columns to appear in the display, select the **Columns to Display** icon in the top right corner of the table.

View API logs

To view REST API logs, navigate to **Logging > APIs**. The **APIs** tab displays REST API requests made during a certain time period.

Be aware of the following considerations:

- REST API logs are cleared after you sign out of the console. (They are also cleared if you refresh your browser window.)
- Any operations in the console that result in API calls have their corresponding API requests displayed on the **APIs** tab.
- The display lists the API requests chronologically (newest entries first), separated by date. The maximum number of API requests in the display is 1,000.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View PowerShell logs

To view PowerShell commands corresponding to UI actions you've taken during the day, navigate to the **Logging > PowerShell** tab.

Associate metadata with configuration logs

You can attach metadata to configuration logs by associating a `name-value` pair called `MetadataMap` with the log records.

NOTE:

- You can only attach metadata to high-level operation objects.
- Metadata is associated with the existing records at the time of execution.

Set the metadata

Run the PowerShell command `Set-LogHighLevelOperationMetadata` to associate a log record with the `MetadataMap`. `Set-LogHighLevelOperationMetadata` takes the following parameters:

- **Id**:ID of the high-level operation.
- **InputObject**:The high-level operations to which you add the metadata. This is an alternative to the `Id` parameter where a high-level operation object or list of objects is passed to the PowerShell command.
- **Name**:Property name of the metadata to be added. The property must be unique for the high-level operation specified. The property cannot contain any of the following characters: `()\/;:#.*?=<>|[]"'`
- **Value**:Value for the property.
- **Map**:Dictionary of (name, value) pairs for the properties. This is an alternative to setting the metadata using the `-Name` and `-Value` parameters.

For example, to attach the metadata to all the high-level log records with Id 40, run the following PowerShell command:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To attach the metadata to the high-level record with the user `abc@example.com`, run the following PowerShell command:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperationMetadata -Name C -Value D
```

Retrieve using the metadata

Run the following PowerShell commands to use the associated metadata to retrieve the log records:

- Search by key and value:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Search by value and any key:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Search by key and any value:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

Remove the metadata

Run the PowerShell command `Remove-LogHighLevelOperationMetadata` to remove the associated metadata. `Remove-LogHighLevelOperationMetadata` takes the following parameters:

- **Id**:ID of the high-level operation.
- **InputObject**:The high-level operations to which you add the metadata. This is an alternative to the `Id`` parameter where a high-level operation object or list of objects is passed to the PowerShell command.
- **Name**:Property name of the metadata to be removed. Set to $null to remove all the metadata for the specified object.
- **Map**:Dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary"). The properties whose names match the keys in the map are removed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Generate reports

To generate a CSV or HTML report containing configuration log data, use PowerShell cmdlets for the ConfigLogging Service in the Citrix Virtual Apps and Desktops Remote PowerShell SDK. For details, see:

- `Export-LogReportCsv`
- `Export-LogReportHtml`

Schedule periodic data deletion

Use the Remote PowerShell SDK to specify how long data is retained in the configuration logging database. (This feature isn't available in Studio.) In Citrix DaaS, you must have Full access.

In the `Set-LogSite` cmdlet, the `-LoggingDBPurgeDurationDays` parameter specifies how many days data is retained in the configuration logging database before it's deleted automatically.

- By default, the value of this parameter is 0. A zero value means that data in the configuration logging database is never deleted automatically.
- When you set a non-zero value, the database is checked once every 120 minutes. Data older than the retention period is deleted.

Use `Get-LogSite` to view the current value of the parameter.

Differences from on-premises Citrix Virtual Apps and Desktops

If you're familiar with configuration logging in the on-premises Virtual Apps and Desktops product, the Citrix Cloud version has several differences. In Citrix Cloud:

- Configuration logging is always enabled. You cannot disable it. Mandatory logging is not available.
- You cannot change the location of the configuration logging database, because the database is managed in the Citrix Cloud platform.
- Configuration log displays do not include operations and activities that are performed within the Citrix Cloud platform.
- PowerShell is your only choice to create a CSV or HTML report of logged operations. In the on-premises product, reports can be generated from Citrix Studio or PowerShell.
- You cannot delete configuration log content.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Delegated administration

Overview

With delegated administration in Citrix Cloud™, you can configure the access permissions that all of your administrators need, in accordance with their role in your organization.

By default, administrators have full access. This setting enables access to all available customer administration and management functions in Citrix Cloud, plus all subscribed services. To tailor an administrator's access:

- Configure custom access for an administrator's general management permissions in Citrix Cloud.
- Configure custom access for subscribed services. In Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service), you can configure custom access when you invite a new administrator. You can change an administrator's access later.

For information about displaying the list of administrators and defining access permissions, see Manage administrator access to Citrix Cloud.

This article describes how to configure custom access in Citrix DaaS.

Administrators, roles, and scopes

Delegated administration uses three concepts for custom access: administrators, roles, and scopes.

- **Administrators:** An administrator represents a person identified by their Citrix Cloud sign-in, which is typically an email address. Each administrator is associated with one or more role and scope pairs.
- **Roles:** A role represents a job function, and has permissions associated with it. These permissions allow certain tasks that are unique to Citrix DaaS. For example, the Delivery Group Administrator role has permission to create a delivery group and remove a desktop from a delivery group, plus other associated permissions. An administrator can have multiple roles. An administrator might be a Delivery Group Administrator and a Machine Catalog Administrator.

  Citrix DaaS offers several built-in custom access roles. You cannot change the permissions within these built-in roles, or delete those roles.

  You can create your own custom access roles to meet your organization's requirements, and delegate permissions with more detail. Use custom roles to allocate permissions at the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

granularity of an action or task. You can delete a customized role only if it is not assigned to an administrator.

You can change which roles an administrator has.

A role is always paired with a scope.

- **Scopes:** A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to your organization. Objects can be in more than one scope.

  There is one built-in scope: All, which contains all objects. Citrix Cloud and Help Desk administrators are always paired with the All scope. That scope cannot be changed for those administrators.

  When you invite (add) an administrator for this service, a role is always paired with a scope (by default, the All scope).

  You create and delete scopes using Studio. You assign role/scope pairs in the Citrix Cloud console.

  A scope is not shown for Full access administrators. By definition, those administrators can access all customer-managed Citrix Cloud and subscribed services objects.

Built-in roles and scopes

Citrix DaaS has the following built-in roles.

- **Cloud Administrator:** Can perform all tasks and operations for managing DaaS.

  Can see the **Manage** and the **Monitor** consoles in Studio. This role is always combined with the All scope. You cannot change the scope.

  Do not be confused by this role's name. A custom access Cloud Administrator cannot perform Citrix Cloud-level tasks (Citrix Cloud tasks require Full access).
- **Read Only Administrator:** Can see all objects in the specified scopes (in addition to global information), but cannot change anything. For example, a Read Only Administrator with a scope of London can see all global objects and any objects in the London scope (for example, London Delivery Groups). However, that administrator cannot see objects in the New York scope (assuming that the London and New York scopes do not overlap).

  Can see the **Manage** and the **Monitor** consoles in Studio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Help Desk Administrator:** Can view delivery groups, and manage the sessions and machines associated with those groups. Can see the machine catalog and host information for the delivery groups being monitored. Can also perform session management and machine power management operations for the machines in those delivery groups.

  Can see the **Monitor** console in Studio. Cannot see the **Manage** console. This role is always combined with the All scope. You cannot change the scope.

- **Machine Catalog Administrator:** Can create and manage machine catalogs and provision the machines into them. Can manage base images and install software, but cannot assign applications or desktops to users.

  Can see the **Manage** and the **Monitor** consoles in Studio. You can change the scope.

- **Delivery Group Administrator:** Can deliver applications, desktops, and machines. Can also manage the associated sessions. Can manage application and desktop configurations such as policies and power management settings.

  Can see the **Manage** and the **Monitor** consoles in Studio. You can change the scope.

  NOTE:

  To change a desktop's display name as a Delivery Group Administrator, you need the **Perform Machine Update** permission. This permission is necessary because changing the display name involves updating the machine property.

- **Host Administrator:** Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to users.

  Can see the **Manage** console in Studio. Cannot see the **Monitor** console. You can change the scope.

- **Session Administrator:** Can view delivery groups being monitored and manage their associated sessions and machines.

  Can see the **Monitor** console in Studio. Cannot see the **Manage** console. You cannot change the scope.

- **Full Monitor Administrator:** Can perform all tasks and operations for monitoring DaaS.

  Can see the **Monitor** console in Studio. Cannot see the **Manage** console. You cannot change the scope.

- **Probe Agent Administrator:** Has access to Probe Agent APIs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Can see the **Manage** and the **Monitor** consoles in Studio. Has read-only access to the **Applications** page but cannot access any other views.

The following table summarizes which console tabs are visible for each custom access role in Citrix DaaS, and whether the role can be used with custom scopes.

CUSTOM ACCESS ADMINISTRATOR ROLE	CAN SEE MANAGE CONSOLE IN STUDIO?	CAN SEE MONITOR CONSOLE IN STUDIO?	CAN ROLE BE USED WITH CUSTOM SCOPES?
Cloud Administrator	Yes	Yes	No
Read Only Administrator	Yes	Yes	Yes
Help Desk Administrator	No	Yes	No
Machine Catalog Administrator	Yes	Yes	Yes
Delivery Group Administrator	Yes	Yes	Yes
Host Administrator	Yes	No	Yes
Session Administrator	No	Yes	No
Full Monitor Administrator	No	Yes	No
Probe Agent Administrator	Yes	Yes	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Custom access administrator roles (except Cloud Administrator and Help Desk Administrator) are unavailable for Virtual Apps Essentials and Virtual Desktops Essentials.
- Custom access administrator roles (except Cloud Administrator and Full Monitor Administrator) are unavailable for Citrix DaaS Standard for Azure.

To view the permissions associated with a role:

1. Sign in to Citrix Cloud.
2. In the **DaaS** tile, click **Manage** to open Studio.
3. In the left pane, select **Manage > Administrators**.
4. Select the **Roles** tab.
5. Select a role in the upper middle pane. The **Role definition** tab in the lower pane lists the categories and permissions. Select a category to see the specific permissions. The **Administrators** tab lists the administrators who have been assigned the selected role.

How many administrators you need

The number of administrators and the granularity of their permissions generally depend on the size and complexity of the deployment.

- In small or proof of concept deployments, one or a few administrators do everything. There is no custom access delegation. In this case, each administrator has Full access, which always has the All scope.
- In larger deployments with more machines, applications, and desktops, more delegation is needed. Several administrators might have more specific functional responsibilities (roles). For example, two have Full access, and others are Help Desk Administrators. Also, an administrator might manage only certain groups of objects (scopes), such as machine catalogs in a particular department. In this case, create new scopes, plus administrators with the appropriate custom access role and scopes.

Administrator management summary

Setting up administrators for Citrix DaaS follows this sequence:

1. If you want the administrator to have a role other than a built-in role, create a custom role.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. If you want the administrator to have a scope other than All (and a different scope is allowed for the intended role, and has not already been created), create scopes.
3. From Citrix Cloud, invite an administrator. If you want the new administrator to have anything other than the default Full access, specify a custom access role and scope pair.

Later, if you want to change an administrator's access (roles and scope), see Configure custom access.

Add an administrator

To add (invite) administrators, follow the guidance in Add administrators to a Citrix Cloud account. A subset of that information is repeated here.

IMPORTANT:

Do not confuse how "custom" and "custom access" are used.

- When creating administrators and assigning roles for Citrix DaaS in the Citrix Cloud console, the term "custom access" includes both the built-in roles and any additional custom roles that were created in the service's Studio interface.
- In the service's Studio interface, "custom" simply differentiates that role from a built-in role.

The general workflow for adding administrators is as follows:

1. Sign in to Citrix Cloud and then select **Identity and Access Management** in the upper left menu.
2. On the **Identity and Access Management** page, select **Administrators**. The **Administrators** tab lists all current administrators for the account.
3. On the **Administrators** tab, select your identity type, enter the administrator's email address, and then click **Invite**.

- Select **Full access** if you want the administrator to have full access. In that way, the administrator can access all customer administrator functions in Citrix Cloud and in all subscribed services.
- Select **Custom access** if you want the administrator to have limited access. You can then select a custom access role and scope pair. In that way, the administrator has the intended permissions when signing in to Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Click **Send Invite**. Citrix Cloud sends an invitation to the email address and adds the administrator to the list after the administrator completes onboarding.

When receiving the email, the administrator clicks the **Sign In** link to accept the invitation.

For more information about adding administrators, see Manage Citrix Cloud administrators.

Alternatively, go to **Administrators > Administrators** in Studio and click **Add Administrator**. You are directly taken to **Identity and Access Management > Administrators**, which opens in a new browser tab. After you are finished adding administrators there, close the tab and return to the console to continue with your other configuration tasks.

Create and manage roles

When administrators create or edit a role, they can enable only the permissions that they themselves have. This control prevents administrators from creating a role with more permissions than they currently have and then assigning it to themselves (or editing a role that they are already assigned).

Custom role names can contain up to 64 Unicode characters. Names cannot contain: backslash, forward slash, semicolon, colon, pound sign, comma, asterisk, question mark, equal sign, left arrow, right arrow, pipe, left or right bracket, left or right parenthesis, quotation marks, and apostrophe.

Role descriptions can contain up to 256 Unicode characters.

1. Sign in to Citrix Cloud if you haven't already.
2. In the **DaaS** tile, click **Manage** to open Studio.
3. In the left pane, select **Manage > Administrators**.
4. Select the **Roles** tab.
5. Follow the instructions for the task you want to complete:

    - **View role details:** Select the role in the middle pane. The lower portion of the middle pane lists the object types and associated permissions for the role. Select the **Administrators** tab in the lower pane to display a list of administrators who currently have this role.
    - **Create a custom role:** Select **Create Role** in the action bar. Configure settings as follows:

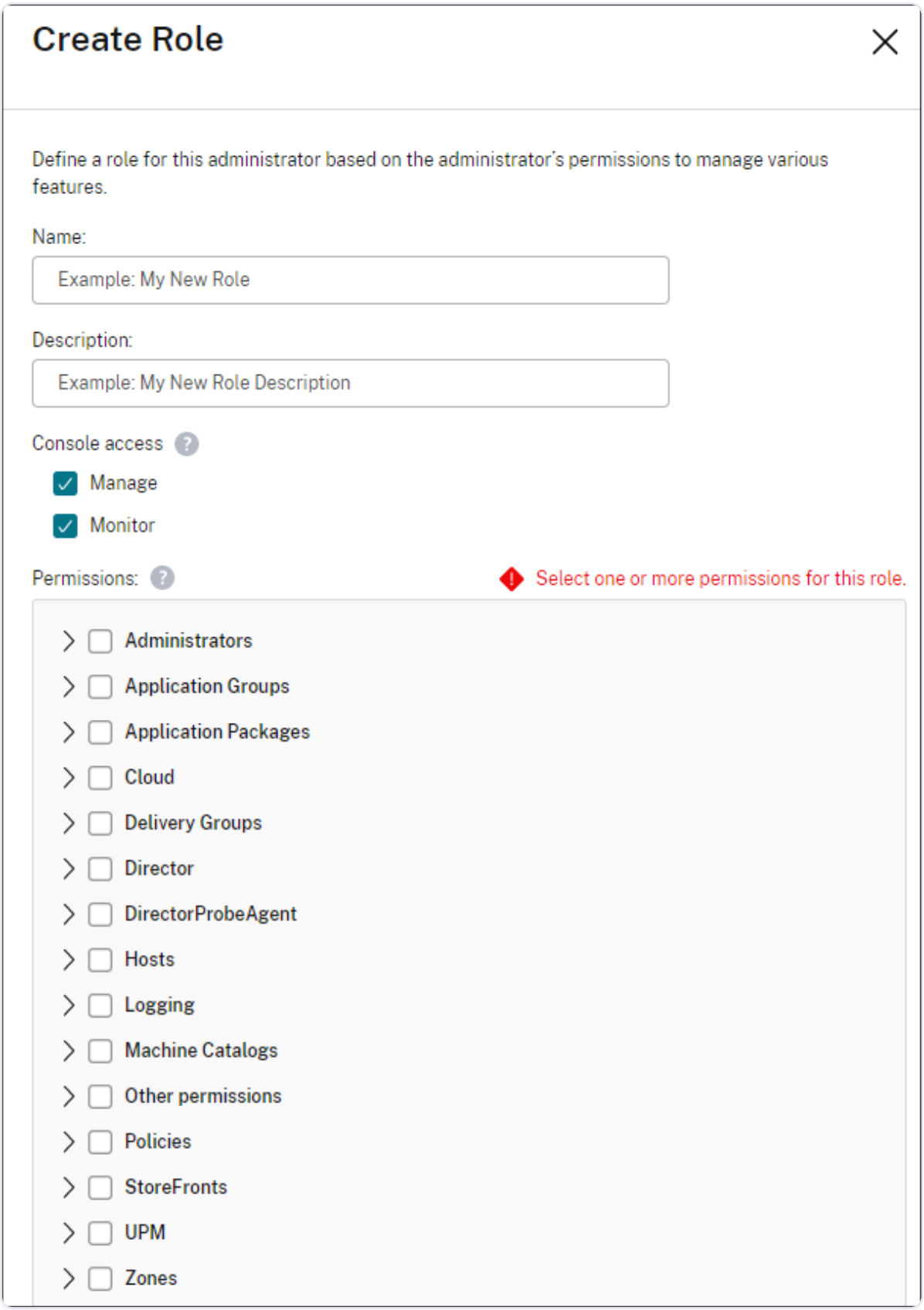
        - Enter a name and description.
        - Configure console access. Determine which consoles are visible to the administrators. You can proceed without selecting any console. In that case, administrators with the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

role cannot access **Manage** and **Monitor** but can access, view, or manage objects through SDKs and APIs.

- Select the object types and permissions. To grant full access permission to an object type, select its check box. To grant permission at a granular level, expand the object type and then select **Read Only** or individual objects under **Manage** within the type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Copy a role:** Select the role in the middle pane and then select **Copy Role** in the action bar. Change the name, description, object types, and permissions, as needed. When you're done, select **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Edit a custom role:** Select the role in the middle pane and then select **Edit Role** in the action bar. Change the name, description, object types, and permissions, as needed. You cannot edit a built-in role. When you're done, select **Save**.
- **Delete a custom role:** Select the role in the middle pane and then select **Delete Role** in the action bar. When prompted, confirm the deletion. You cannot delete a built-in role. You cannot delete a custom role if it is assigned to an administrator.

Create and manage scopes

By default, all roles have the All scope for their relevant objects. For example, a Delivery Group Administrator can manage all Delivery Groups. For some administrator roles, you can create a scope that allows that administrator role to access a subset of the relevant objects. For example, you might want a give a Machine Catalog Administrator access to only catalogs that contain a certain type of machines, rather than all catalogs.

- Full access administrators or custom access Cloud Administrators can create scopes for the Read Only Administrator, Machine Catalog Administrator, Delivery Group Administrator, and Host Administrator roles.
- Scopes cannot be created for Full access administrators, nor can they be created for Cloud Administrators or Help Desk Administrators. Those administrators always have the All scope.

Create scopes

1. In Studio, select **Manage > Administrators** in the left pane.
2. Select the **Scopes** tab.
3. In the action bar, select **Create Scope**.
4. Enter a name and description:
    - Scope names can contain up to 64 Unicode characters. Names cannot include: backslash, forward slash, semicolon, colon, pound sign, comma, asterisk, question mark, equal sign, left or right arrow, pipe, left or right bracket, left or right parenthesis, quotation marks, and apostrophe.
    - Scope descriptions can contain up to 256 Unicode characters.
5. Select the objects that you want to include in this scope. Objects are listed by type, such as delivery groups and machine catalogs.
    - To include all objects of a particular type (for example, all delivery groups), select the check box for the object type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To include individual objects within a type, expand the type and then select the check boxes for the objects (for example, specific delivery groups).

  NOTE:

  Application groups, delivery groups, or machine catalogs are displayed in folder structures that align with their management in DaaS. You can select a folder to select all its objects or expand a folder to select specific objects.

- To include an object that previously didn't support scope control (an *unscoped* object) and now supports it (a *scoped* object), disable **Bypass scope control** next to the object, and then select it.

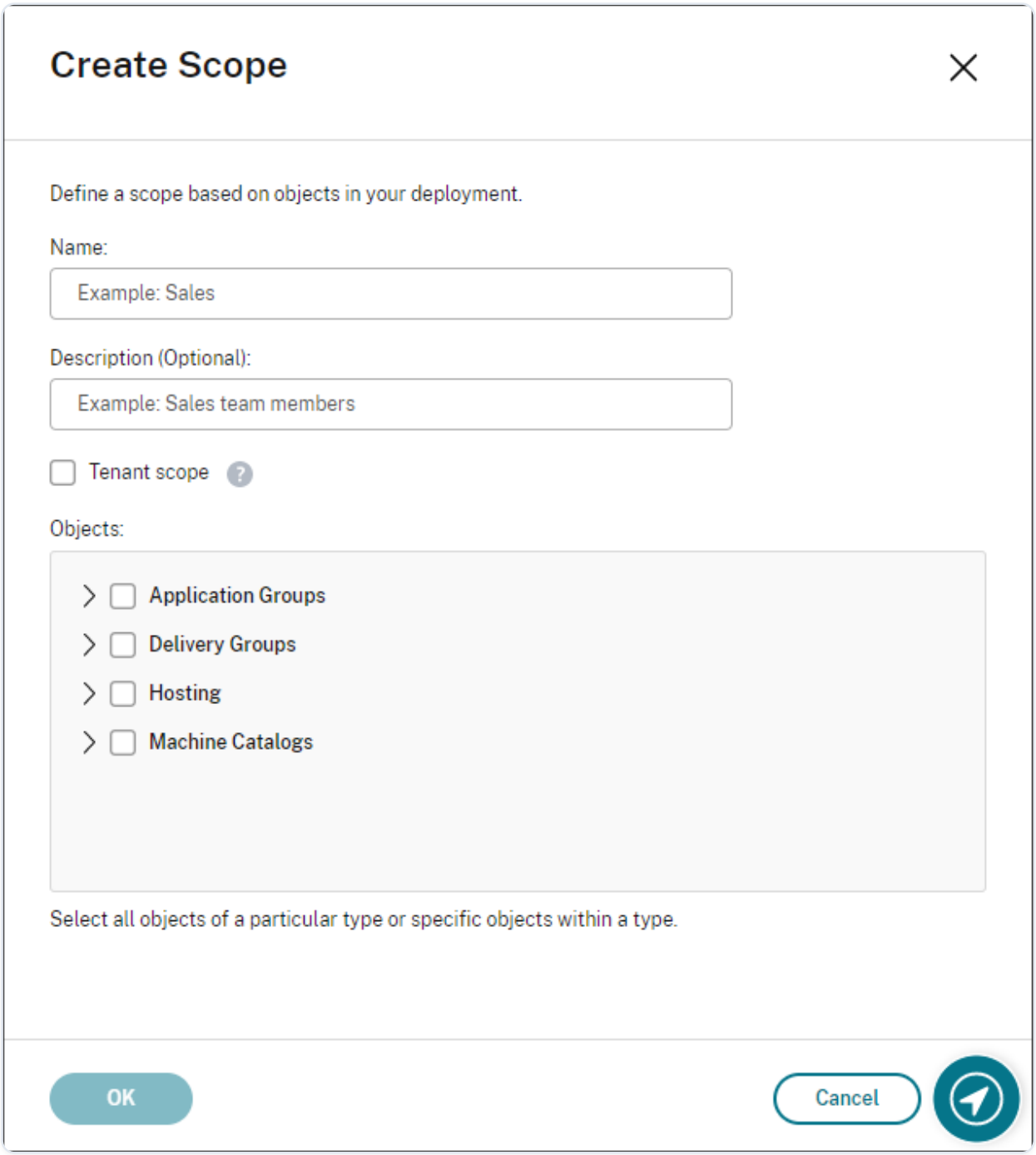
  NOTE:

  Unscoped objects are visible to all administrators with the required permissions. When such an object becomes *scoped*, **Bypass scope control** appears and is enabled by default to preserve visibility to all administrators.

- To create a tenant customer, select the **Tenant scope** check box. If selected, the name you entered for the scope is the tenant name. For more information about the tenant scope, see Manage tenants.

6. When you're done, select **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After you create a scope, it appears in the **Custom access** list in the Citrix Cloud console. You can then select it when you assign a role to an administrator.

For example, if you create a scope named **CAD** and include catalogs with machines suitable for CAD applications, the **CAD** scope appears in the **Edit scopes** list when you assign roles in the Citrix Cloud console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The **Cloud Administrator** and **Help Desk Administrator** roles always have the **All** scope. The CAD scope doesn't apply to them.

Manage scopes

You can perform the following tasks to manage scopes:

- **View scope details:** Select the scope. The lower portion of the pane lists the objects and administrators that have that scope.
- **Copy a scope:** Select the scope in the middle pane and then select **Copy Scope** in the action bar. Change the name, description. Change the object types and objects, as needed. When you're done, select **Save**.
- **Edit a scope:** Select the scope in the middle pane and then select **Edit Scope** in the action bar. Change the name, description, object types, and objects, as needed. When you're done, select **Save**.

  NOTE:

  When you copy or edit a scope, keep in mind that removing objects from the scope can make those objects inaccessible to an administrator. If the edited scope is paired with one or more roles, ensure that your scope updates do not make any role/scope pair unusable.

- **Delete a scope:** Select the scope in the middle pane and then select **Delete Scope** in the action bar. When prompted, confirm the deletion.

  You cannot delete a scope if it is assigned to a role. If you attempt to do this, an error message indicates that you do not have permission. In fact, the error occurs because the role/scope pair that uses this scope is assigned to an administrator. First, remove the role/scope pair assignment for all administrators who use it. Then delete the scope in Studio.

Manage tenants

Using Studio, you can create mutually exclusive tenants under a single Citrix DaaS. You achieve that by creating tenant scopes in **Administrators > Scopes** and associating related configuration objects, such as machine catalogs and delivery groups, with those tenants. As a result, administrators with access to a tenant can manage only objects that are associated with the tenant.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

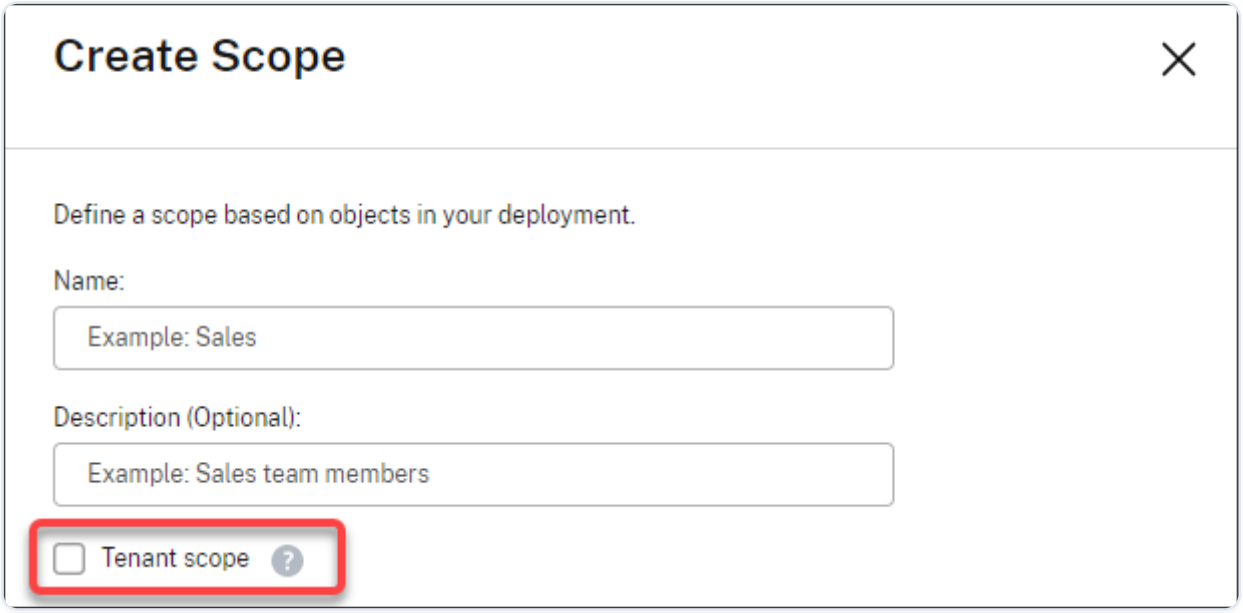
This feature is useful, for example, if your organization:

- Has different business silos (independent divisions or separate IT management teams) or
- Has multiple on-premises sites and wants to maintain the same setup in a single Citrix DaaS instance.

The interface lets you filter tenant customers by name. By default, the interface displays information about all tenant customers. To display information about a specific tenant, select that tenant from the list in the upper-right corner.

Create a tenant customer

To create a tenant customer, select **Tenant scope** when creating a scope. By selecting the option, you create a unique scope type that applies to objects in scenarios where you share a Citrix DaaS instance between different business units— each of those business units are independent of the others. After you create a tenant scope, you cannot change the scope type.



The **Scopes** tab displays all scope items. The only difference between regular scopes and tenant scopes is in the **Type** column. A blank column field indicates a regular scope. You can click the **Type** column to sort scope items if needed.

To see the resources (objects) attached to a scope, select **Administrators** in the left pane. On the **Scopes** tab, select the scope and then select **Edit Scope** in the action bar.

TIP:

The tenant property is assigned at a scope level. Machine catalogs, delivery groups, applications, and connections inherit the tenant property from the applicable scope.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

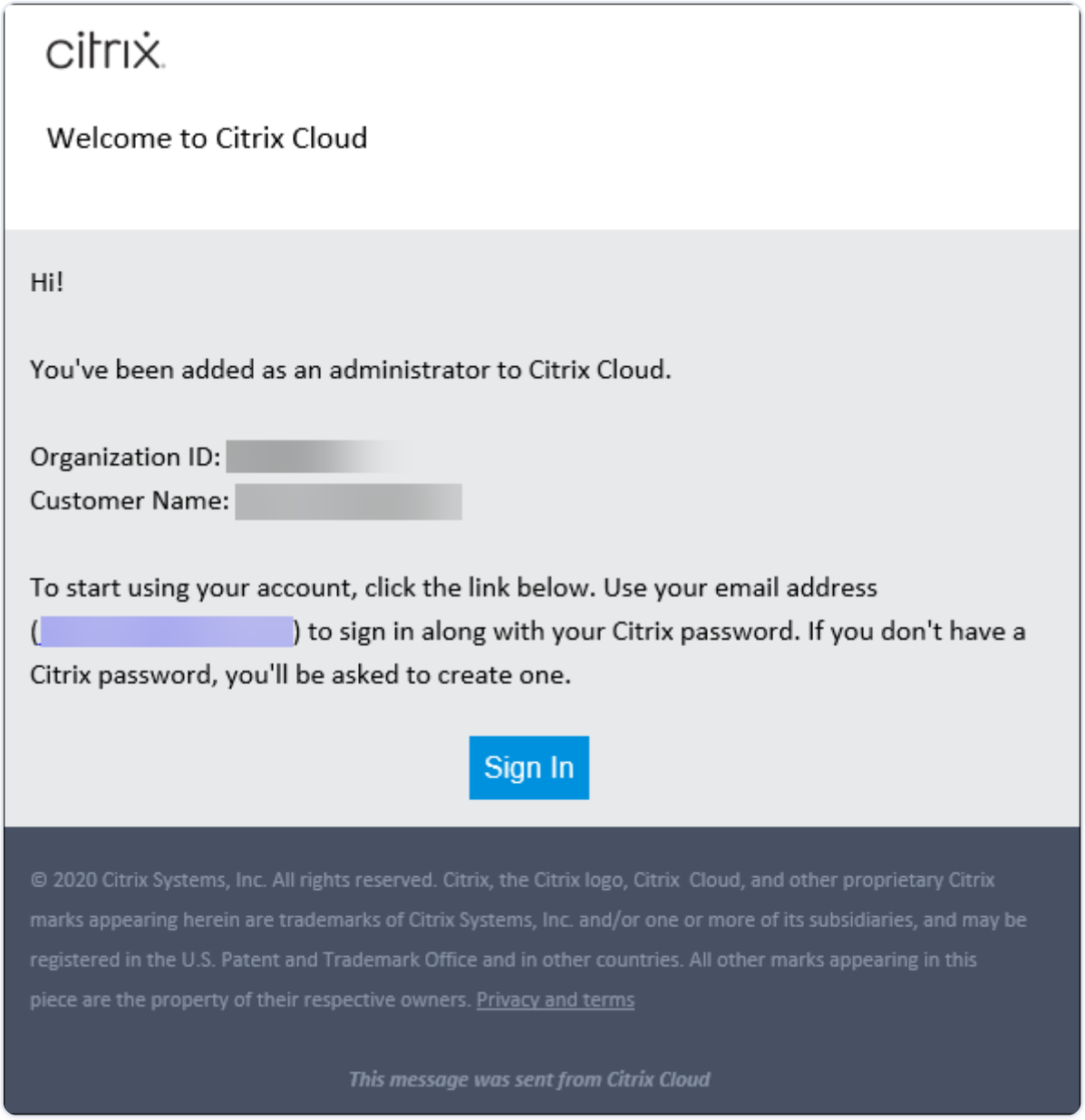
When using a tenant scope, be aware of the following considerations:

- The tenant property is assigned in the following order: **Hosting > Machine Catalogs > Delivery Groups > Applications**. Lower-level objects rely on higher-level objects to inherit the tenant property from. For example, when selecting a delivery group, you must select the associated hosting and machine catalog. Otherwise, the delivery group cannot inherit the tenant property.
- After creating a tenant scope, you can edit tenant assignments by modifying objects. When a tenant assignment is changed, it is still subject to the constraint that it must be assigned to the same tenants or to a subset of those tenants. However, lower-level objects are not reevaluated when tenant assignments change. Make sure that objects are properly restricted when you change tenant assignments. For example, if a machine catalog is available for `TenantA` and `TenantB`, you can create a delivery group for `TenantA` and one for `TenantB`. (`TenantA` and `TenantB` are both associated with that machine catalog.) You can then change the machine catalog to be associated only with `TenantA`. As a result, the delivery group associated with `TenantB` becomes invalid.

Configure custom access for administrators

After creating tenant scopes, configure custom access for respective administrators. For more information, see Configure custom access for an administrator. Citrix Cloud sends an invitation to those customer administrators you specified and adds them to the list. When they receive the email, they click **Sign In** to accept the invitation. When they sign in to Studio, they see resources that the assigned role and scope pairs contain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Administrators with access to a tenant can manage only objects (for example, machine catalog, delivery group) that are associated with the tenant.

Configure custom access for an administrator

This feature lets you define access permissions of existing administrators or administrators you invite in a way that aligns with their role in your organization.

Changes you made to access permissions take 5 minutes to take effect. Signing out of Studio and logging back on makes the changes take effect immediately. In scenarios where administrators still use the management interface after the changes take effect without reconnecting to it, a warning appears when they attempt to access items to which they no longer have permissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

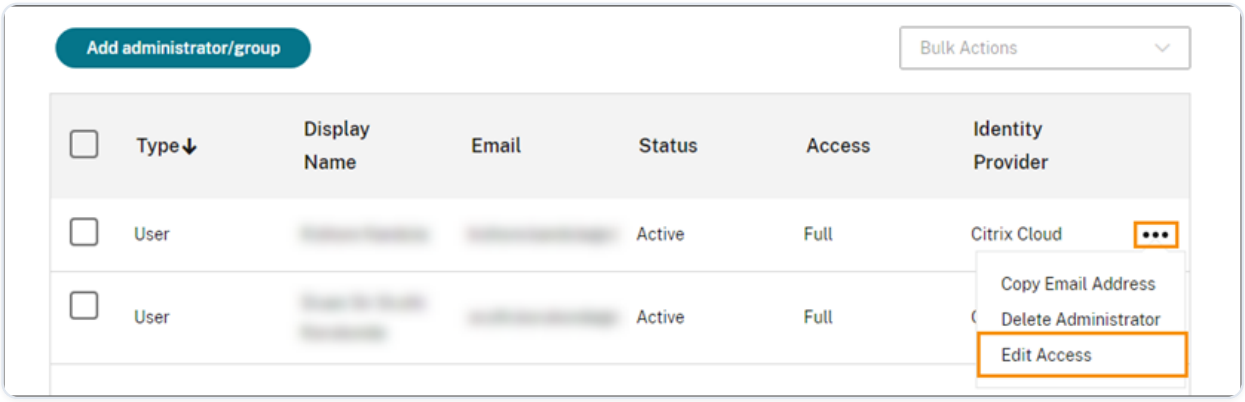
By default, when you invite administrators, they have Full access. Full access allows the administrator to manage all subscribed services and all Citrix Cloud operations (such as inviting more administrators). A Citrix Cloud deployment needs at least one administrator with Full access.

You can also grant custom access when you invite an administrator. Custom access allows the administrator to manage only the services and operations that you specify.

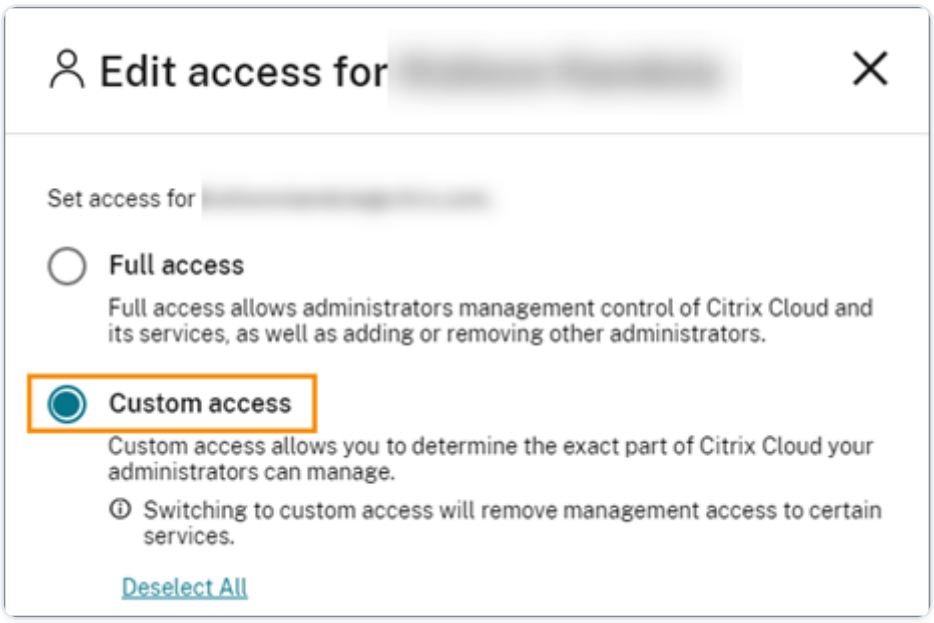
When you create a role or scope in Citrix DaaS, it appears in the custom access list and can be selected. When you select a role for an administrator, you can modify the scopes as needed to reflect the administrator's role in your organization.

To configure custom access for an administrator:

1. Sign in to Citrix Cloud. Select **Identity and Access Management** > **Administrators** in the upper left menu.
2. Locate the administrator you want to manage, select the ellipsis menu, and select **Edit access**.

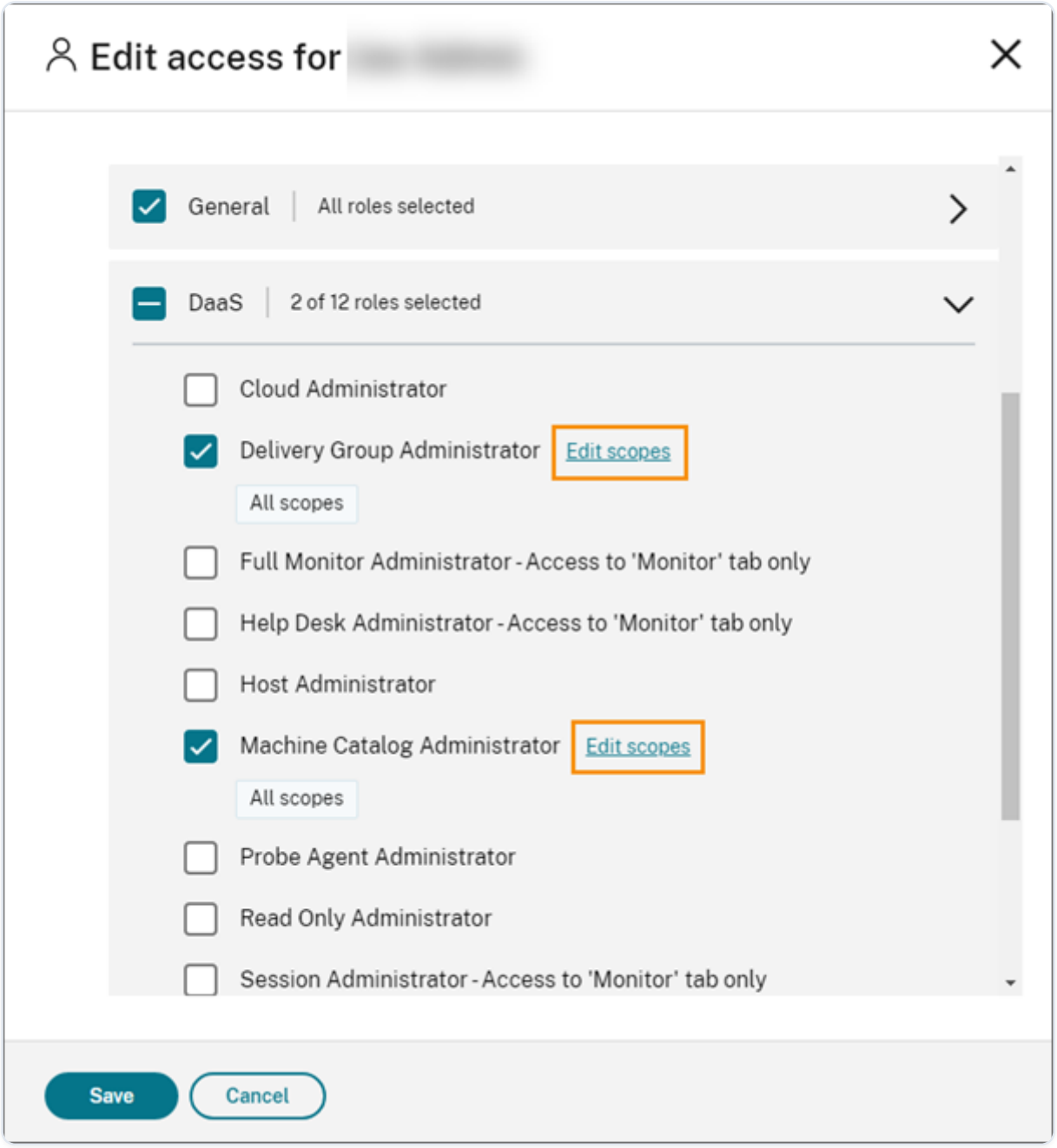


3. Select **Custom access**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

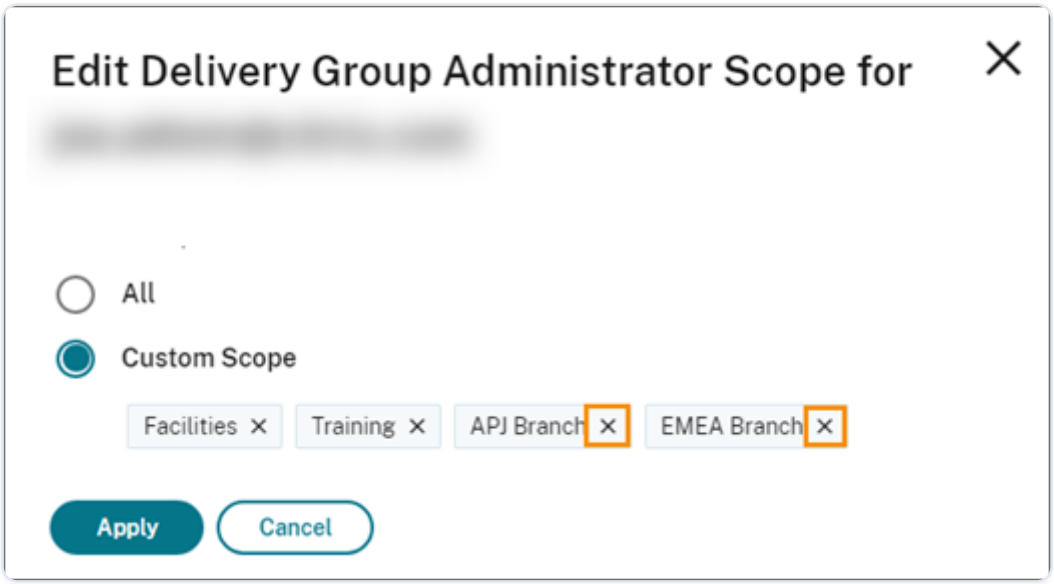
4. Under **DaaS**, select or clear the check marks next to one or more roles. To modify the scopes associated with an assigned role, select **Edit scopes**.



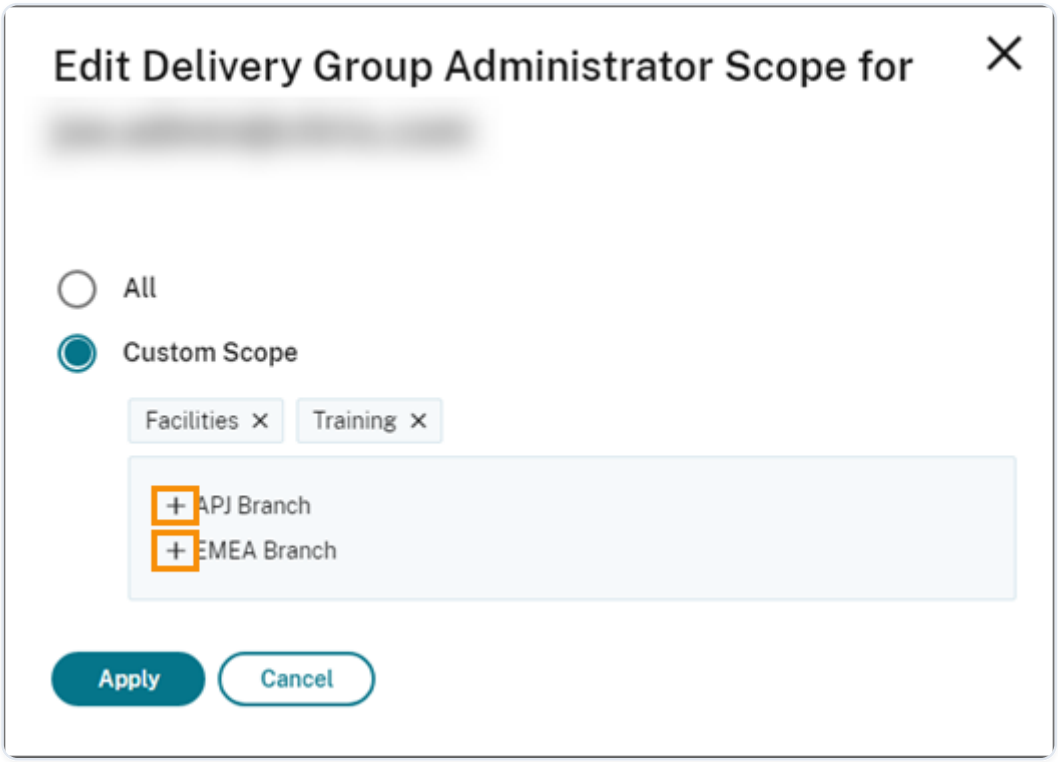
By default, each selected role has all scopes selected, as noted by the **All scopes** label.

5. To specify the scopes for a selected role, select **Custom Scope** and then add or remove the appropriate scopes. By default, all custom scopes are added to a role. To remove a scope, click the X icon on the scope.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Scopes that have been removed and are available to add to the role appear in a list below the scopes that are already added. To add a scope to the role, select the plus icon for the scope.



6. When you're finished selecting scopes, select **Apply**.
7. Select **Save** to save the selected roles for the administrator.

Differences from on-premises Citrix Virtual Apps and Desktops

If you're familiar with delegated administration in the on-premises Citrix Virtual Apps and Desktops product, Citrix DaaS version has several differences.

In Citrix Cloud:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Administrators are identified by their Citrix Cloud login, rather than their Active Directory account. You can create role/scope pairs for Active Directory individuals, but not groups.
- Administrators are created, configured, and deleted in the Citrix Cloud console, rather than Citrix DaaS.
- Role/scope pairs are assigned to administrators in the Citrix Cloud console, rather than Citrix DaaS.
- Reports are not available. You can view administrator, role, and scope information in the service's Studio interface.
- The custom access Cloud Administrator is similar to a Full Administrator in the on-premises version. Both have full management and monitoring permissions for the Citrix Virtual Apps and Desktops version being used.

  However, in Citrix DaaS, there is no named Full Administrator role. Do not equate "Full access" in Citrix Cloud with the "Full administrator" in on-premises Citrix Virtual Apps and Desktops. Full access in Citrix Cloud spans the platform-level domains, library, notifications, and resource locations, plus all subscribed services.

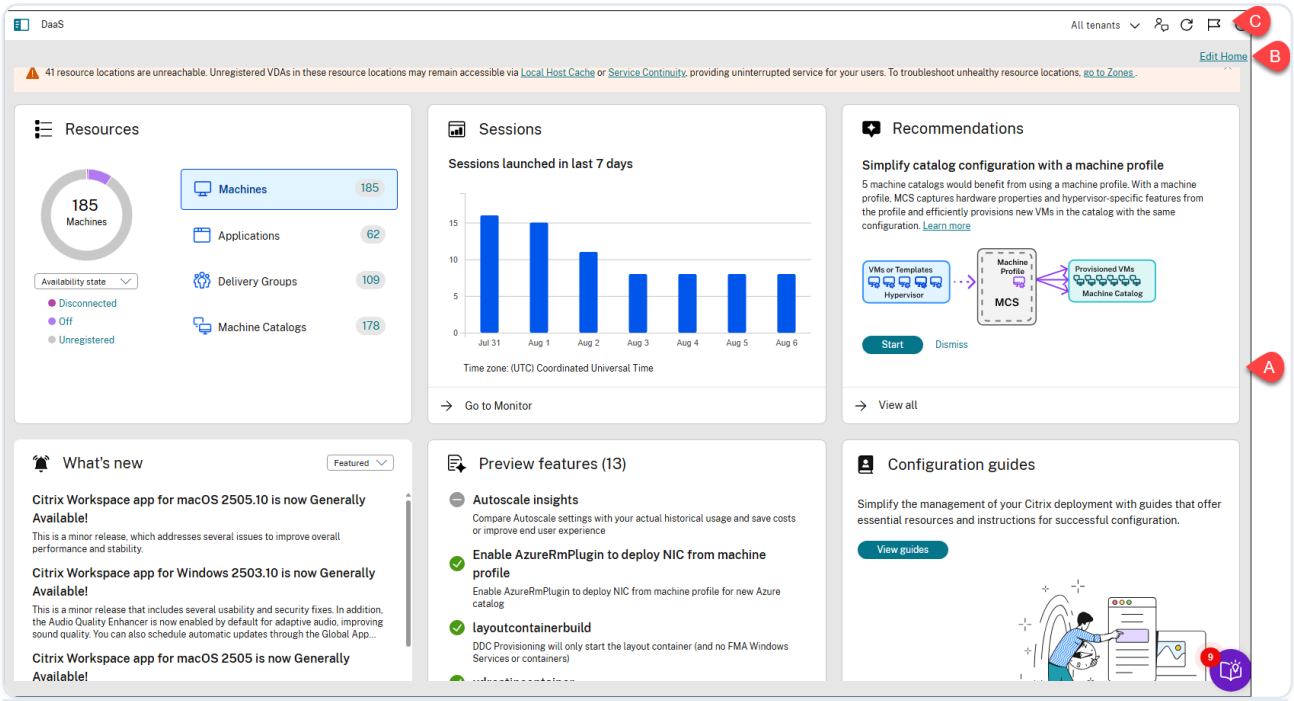
More information

See Delegated administration and monitoring for information about administrators, roles, and scopes used in the service's **Monitor** node.

Home page

The Studio Home page provides an overview of your Citrix DaaS™ deployment and workloads along with information that helps you get the most from your subscription. This article introduces the available widgets on this page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



CALLOUT	AREA	DESCRIPTION
A	Widgets	Provides an overview of your Citrix DaaS deployment and workloads, along with information that helps you get the most from your subscription. Widgets include Resources, Sessions, Recommendations, What's new, Preview features, Configuration guides, Errors and warnings, and Advisor.
B	Edit Home action	Lets you customize the Home page by adding, removing, or repositioning widgets.
C	Service health alerts (flag icon)	Displays alerts related to your site's health.

Resources

This widget provides an overview of your Citrix DaaS deployment:

- **Resources**. Shows the numbers of deployed resources and their counts by category.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESOURCE	TO VIEW COUNTS BY CATEGORY
Machines	Click **Machines**, select a state, and then hover over the donut chart for details. Available options: **Availability state** (Available, In use, Off, and Unavailable), **Registration state** (Registered and Unregistered), and **Maintenance state** (In maintenance and Not in maintenance). When viewing machine counts by availability state, you can click a state to view the corresponding machine details.
Applications	Click **Applications** and hover over the donut chart for details.
Delivery Groups	Click **Delivery Groups** and hover over the donut chart for details.
Machine Catalogs	Click **Machine Catalogs** and hover over the donut chart for details.

- **Sessions launched in last 7 days**. Shows the number of desktop and app sessions launched each day for the last seven days. To drill down for more details, click Go to Monitor.

Sessions

This widget provides an overview of your Citrix DaaS workloads in the last 7 days. Shows the number of desktop and app sessions launched daily over the previous seven days. To drill down for more details, click Go to Monitor.

Recommendations

This widget recommends features that are available with your subscription, such as Workspace Environment Management and Autoscale. To engage with us, like or dislike a recommendation and leave your feedback.

NOTE:

If you dislike a recommendation, the recommendation disappears. If you dislike all recommendations or the recommendation widget, the recommendation widget disappears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

This widget shows a select list of the latest Citrix DaaS features that are most valuable to your business. Using those features helps you get the most from your subscription. For a complete list of new features, see What's new.

Preview features

This widget shows features that are currently in preview. As a Citrix Cloud™ administrator with full access, you can turn preview features on or off without contacting Citrix. It takes up to 15 minutes for the changes to take effect.

Preview features are recommended for use in non-production environments. Issues found with preview features aren't supported by Citrix Technical Support.

Configuration guides

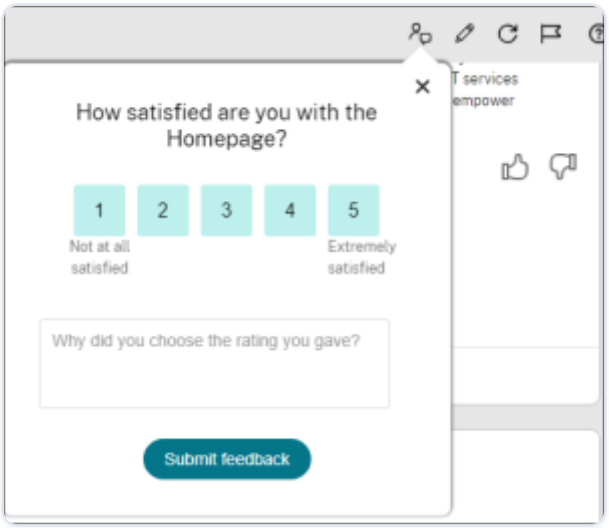
This widget provides step-by-step guidance for configuring and managing various aspects of your Citrix deployment:

- **Get started with DaaS**. Guides you through a series of questions to help you set up your DaaS deployments. By answering these questions, you can quickly configure your deployments. For more information, see Use DaaS get-started guide.
- **Check resiliency configurations**. Guides you through verifying that your Citrix DaaS deployment is properly set up to handle potential disruptions. This guide provides checklists to verify that key components, such as Local Host Cache and Service Continuity, are correctly configured. This verification helps ensure uninterrupted access to apps and desktops during service interruptions. It includes checklists for verifying resiliency settings across various StoreFront™ deployment types:
  - Checklist for on-premises Citrix® StoreFront deployments
  - Checklist for Citrix® StoreFront Cloud deployments
  - Checklist for mixed StoreFront deployments

NOTE:

The resilience checklist isn't a one-time task. We encourage you to regularly review your resiliency readiness by testing Service Continuity and Local Host Cache. If you have feedback on the checklist, use the feedback icon in the top-right corner of the Home page to share it with us.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Errors and warnings

Centrally displays errors and warnings from your DaaS deployments:

- Lists the number of errors and the number of warnings present in the following configuration nodes: Zones, Machines, Machine Catalogs, Delivery Groups, Hosting, and Images. Clicking a number links you to the UI of the corresponding node.
- Lists the high-priority errors in your site, along with recommended actions.

Advisor

The **Advisor** widget displays a summary of recommendations from your most recent Advisor site check, giving you quick visibility into environment health without leaving the Home page.

The widget shows:

- A count of total recommendations grouped by impact level: **High**, **Medium**, and **Low**
- A visual bar chart showing the distribution across impact levels
- A filterable list of recommendations by category: **Security**, **Reliability**, **Performance**, **Operational Excellence**, and **Cost Optimization**
- A timestamp indicating when Advisor last ran

You can filter recommendations by selecting a category from the drop-down menu. Select any recommendation in the list to navigate directly to its details in the full **Advisor** page. Select **Go to Advisor** to view the complete Advisor interface.

If no recent check results are available, the widget displays a message prompting you to run a new site check.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customize the Home page

To customize the Home page, follow these steps:

1. Sign in to Citrix Cloud.
2. In the **DaaS** tile, click **Manage**. The home page appears.
3. Click the **Edit** icon in the top right corner of the Home page.
4. To reposition a widget, drag it to a wanted position.
5. To remove a widget from the Home page, click the **Delete** icon in the top right of the widget.
6. To add a widget back to the Home page, click the **Add widget** icon in the top right corner of the Home page.
7. Click **Done** to save changes.

Licenses

This article covers tasks and resources for Microsoft licenses and Citrix® licenses.

Configure a Microsoft RDS License Server for Windows Server workloads

This information applies when you are delivering Windows Server workloads.

This service accesses Windows Server remote session capabilities when delivering a Windows Server workload, such as Windows 2019. This typically requires a Remote Desktop Services client access license (RDS CAL). The VDA must be able to contact an RDS license server to request RDS CALs.

Install and activate the license server. For more information, see the Microsoft document Activate the Remote Desktop Services License Server. For proof of concept environments, you can use the grace period provided by Microsoft.

With this method, you can have this service apply the license server settings. You can configure the license server and per user mode in the RDS console on the image. You can also configure the license server using Microsoft Group Policy settings. For more information, see the Microsoft document License your RDS deployment with client access licenses (CALs).

To configure the RDS license server using Microsoft Group Policy settings:

1. Install a Remote Desktop Services License Server on an available VM. The VM must always be available. The Citrix service workloads must be able to reach this license server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Specify the license server address and per-user license mode using Microsoft Group Policy. For details, see the Microsoft document Specify the Remote Desktop Licensing Model for an RD Session Host Server.

Windows 10 workloads require appropriate Windows 10 license activation. We recommend that you follow Microsoft documentation to activate Windows 10 workloads.

Citrix license usage

For information about Citrix license usage, see:

- Monitor license and active usage for cloud services
- Monitor license and active usage for Citrix DaaS

Local Host Cache

This article provides a complete overview of the Local Host Cache (LHC) feature, focusing on its ability to maintain business continuity. It explains the functionality of LHC both during normal working operations and when LHC mode activates. Additionally, the article offers guidance on configuration checks, troubleshooting, PowerShell commands for LHC management, and event log monitoring for LHC health.

Overview

LHC maintains end user access to apps and desktops when Cloud Connectors lose connectivity with Citrix Cloud™ due to a network disruption or an issue with Citrix Cloud. Active sessions are not impacted when LHC mode activates and new sessions are brokered through the LHC broker running on the Cloud Connectors.

LHC is enabled by default, but it is important to ensure that your environment is configured properly for LHC. While misconfigurations might not disrupt normal brokering, they can hinder LHC performance causing disruption to end users when LHC mode is active. To ensure optimal LHC functionality, check your Zones node in Studio for zone-related errors and warnings that Citrix has detected. Additionally, review the Check resiliency configurations guide and the Avoid Common Misconfigurations that Can Negatively Impact DaaS Resiliency article for a comprehensive LHC configuration checklist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

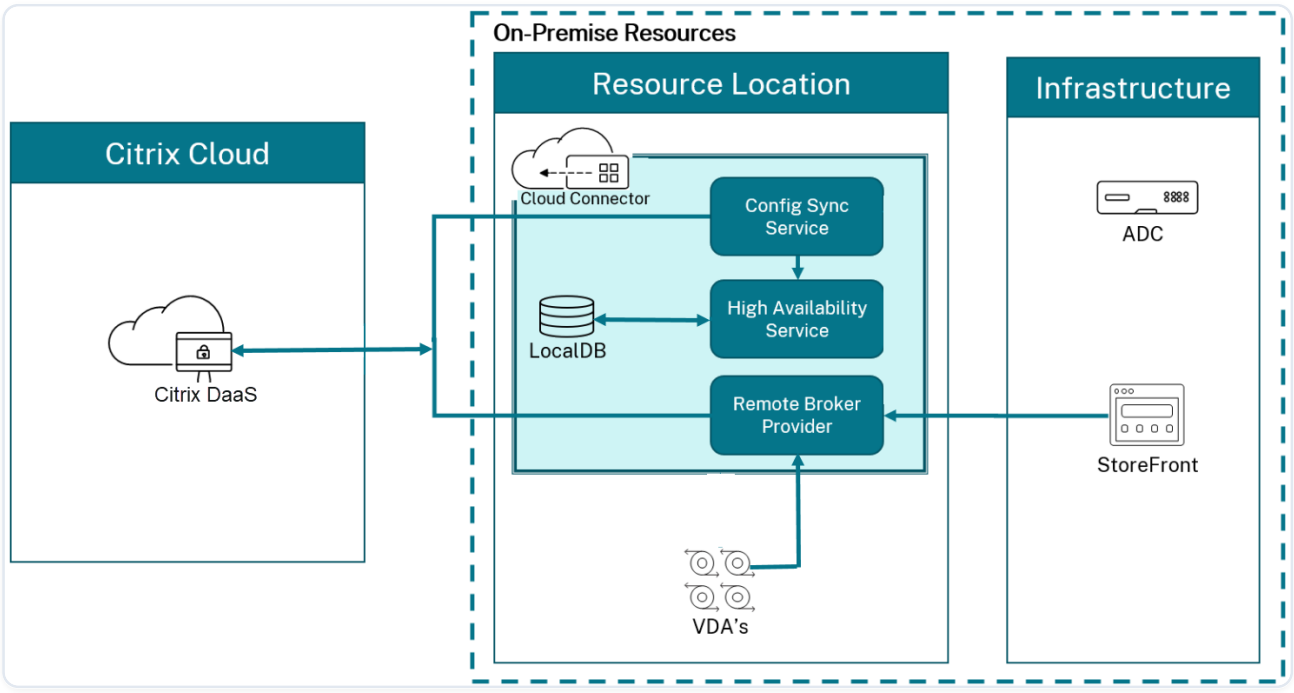
IMPORTANT:

LHC only engages if Cloud Connectors receive traffic from StoreFront or if Service Continuity is enabled. For more information on how Service Continuity can use Local Host Cache to maintain user access to apps and desktops during service disruptions, see Service continuity.

How it works

During normal operations, the Remote Broker Provider Service on a Cloud Connector communicates with Citrix Cloud for all brokering operations. The Citrix Config Synchronizer Service (CSS) regularly checks for configuration changes in Citrix Cloud and synchronizes this data to the LHC broker on the Cloud Connector. If Cloud Connectors lose connectivity to Citrix Cloud or Citrix Cloud is experiencing an issue, then LHC mode activates and ensures continued access to applications and desktops.

During normal brokering operation



- The Citrix Remote Broker Provider Service on a Cloud Connector accepts connection requests from StoreFront. The Remote Broker Provider Service communicates with Citrix Cloud to connect users with VDAs that are registered with Citrix Cloud.
- The CSS checks with the Cloud broker in Citrix Cloud approximately every 5 minutes to see if any configuration changes were made. Those changes can be administrator-initiated (such as changing a delivery group property) or system actions (such as machine assignments).

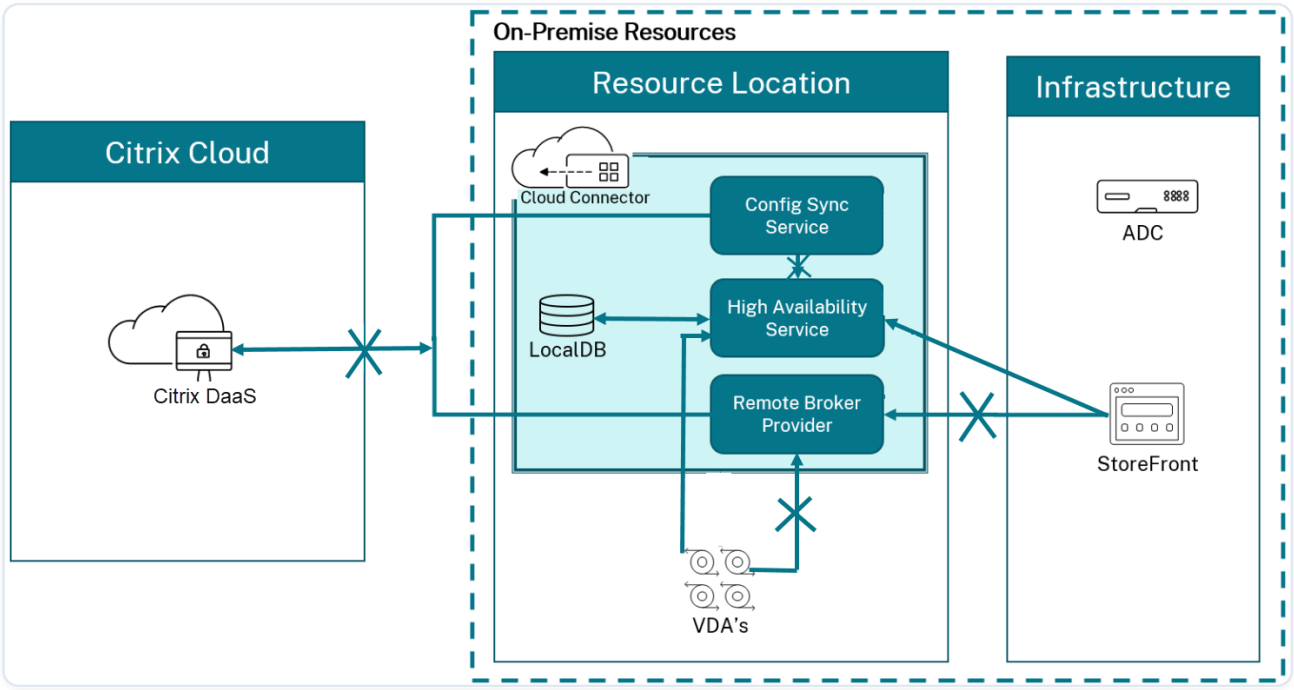
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If a configuration change occurred since the previous check, CSS synchronizes information to the LHC broker on the Cloud Connector. (The LHC broker is also referred to as the High Availability Service, or HA broker).

  All configuration data is copied, not just items that changed since the previous check. The CSS imports the configuration data into a Microsoft SQL Server Express LocalDB database on the Cloud Connector. This database is referred to as the Local Host Cache database. The CSS ensures that the information in the Local Host Cache database matches the information in the site database in Citrix Cloud.

  Microsoft SQL Server Express LocalDB (used by the LHC database) is installed automatically when you install a Cloud Connector. The LHC database cannot be shared across Cloud Connectors. You do not need to back up the LHC database. It is recreated every time a configuration change is detected.
- If no changes occurred since the last check, the configuration data is not copied.

When LHC mode becomes active



- The LHC broker starts listening for connection information and processing connection requests.
- When the Cloud Connectors first lose connectivity to Citrix Cloud, the LHC broker does not have current VDA registration data, but when a VDA communicates with it, a registration process is triggered. During that process, the LHC broker also gets current session information for that VDA.
- While the LHC broker is handling connections, the Remote Broker Provider Service continues to monitor the connection to Citrix Cloud. When the connection is restored, the Remote Broker

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Provider Service instructs the LHC broker to stop listening for connection information, and Citrix Cloud resumes brokering operations. The next time a VDA communicates with Citrix Cloud through the Remote Broker Provider Service, a registration process is triggered. The LHC broker removes any remaining VDA registrations from when LHC mode was active. The CSS resumes synchronizing information when it learns that configuration changes have occurred in Citrix Cloud.

In the unlikely event that LHC begins during a synchronization, the current import is discarded and the last known configuration is used.

The event log indicates when synchronizations occur and LHC mode activates.

There is no time limit imposed for operating in LHC mode.

You can also manually trigger LHC mode. See Force LHC mode for details about why and how to do this.

Zones with multiple Cloud Connectors

Among other tasks, the CSS routinely provides the LHC broker with information about all Cloud Connectors in the zone. Having that information, each LHC broker knows about all peer LHC brokers running on other Cloud Connectors in the zone.

The LHC brokers communicate with each other on a separate channel. Those brokers use an alphabetical list of FQDN names of the machines that they're running on to determine (elect) which LHC broker will broker operations in the zone if the zone enters LHC mode. During LHC mode, all VDAs re-register with the elected LHC broker. The non-elected LHC brokers in the zone actively reject incoming connection and VDA registration requests.

IMPORTANT:

Connectors within a zone must be able to reach each other at `http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection`. If Connectors cannot communicate at this address, multiple brokers might be elected and launch failures occur when in LHC mode.

During LHC mode, if a Cloud Connector is restarted or the LHC broker fails:

- If that Cloud Connector is not the elected LHC broker, the restart has no impact.
- If that Cloud Connector is the elected LHC broker, the LHC broker on the next Cloud Connector is elected, causing VDAs to register. Election order is based on the alphabetical order of the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FQDN of Cloud Connectors. Once the LHC broker becomes active again, LHC operations continue on the first connector in alphabetical order, which can cause VDAs to register again. In this scenario, performance can be affected during the registrations.

See event logs for more information regarding events pertaining to LHC broker elections.

Local Host Cache data content

The LHC database includes the following data, which is a subset of the data in the main database:

- Identities of users and groups who are assigned rights to resources published from the site.
- Identities of users who are currently using, or who have recently used, published resources from the site.
- Identities of VDA machines (including Remote PC Access machines) configured in the site.
- Identities (names and IP addresses) of client Citrix Workspace™ app machines being actively used to connect to published resources.

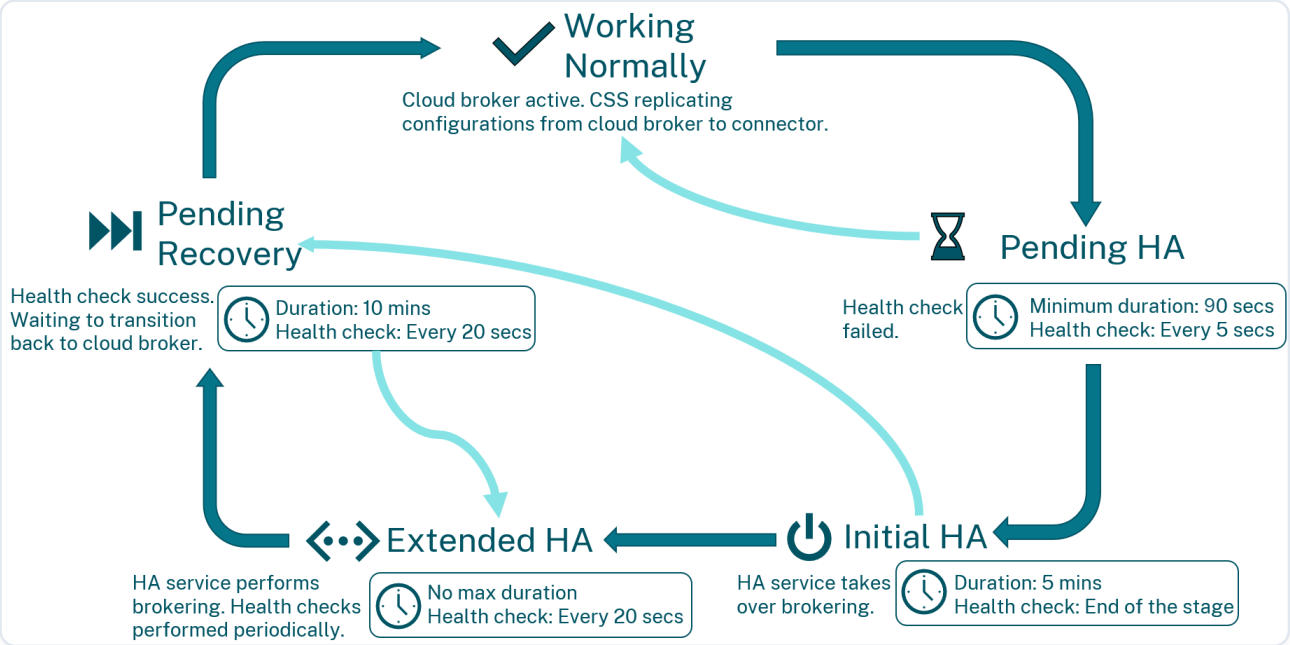
It also contains the following information for currently active connections that were established while in LHC mode:

- Results of any client machine endpoint analysis performed by Citrix Workspace app.
- Identities of infrastructure machines (such as Citrix Gateway and StoreFront servers) involved with the site.
- Dates, times, and types of recent activity by users

Local Host Cache states

There are several states during the entire cycle of entering and exiting LHC mode. The following diagram describes the states for entering and exiting LHC mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- During the **Working Normally** state, all components are healthy and all brokering transactions are handled by the Cloud broker. - - The CSS is actively replicating the configurations from the Cloud broker to the Cloud Connectors. If any health checks fail, Cloud Connectors transitions to the **Pending HA** state. When in this state, a comprehensive health check is initiated to determine the next course of action. The connectors interact with other connectors in the zone to determine their health status.
- The decision to move from **Pending HA** to **Initial HA** is based on the health status of all the connectors in a given zone. If the health checks are successful, the connectors/controllers transition back to the **Working Normally** state. Alternatively, if the health checks continue to fail, the connectors/controllers transition to the **Initial HA** state.
- During the **Initial HA** state, the LHC broker on the elected connector takes over brokering responsibilities. All VDAs in the current zone that were registered before will now register with the LHC broker on the Cloud Connector. It can take up to 5 minutes for all VDAs to re-register with the HA Service. At the end of **Initial HA**, health checks are initiated. If all health checks succeed, the state transitions to **Pending Recovery**, otherwise the state transitions to **Extended HA**.
- Health checks continue to occur during the **Extended HA** period. When health checks succeed during the **Extended HA**, the state transitions to **Pending Recovery**. There is no maximum time duration for a connector to remain in the **Extended HA** state.
- **Pending Recovery** serves as a buffer period to ensure that services are fully healthy before transitioning out of LHC mode. If any of the health checks fail during **Pending Recovery**, the state transitions back to **Extended HA**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If all the health checks succeed during the entirety of the 10-minute **Pending Recovery** period, then the state transitions to **Working Normally**. With this transition, LHC mode ends, and all the VDAs in the zone that were registered with the LHC broker now re-register with the Cloud broker. This re-registration can again take up to 5 minutes.

Important considerations during LHC mode

During LHC mode, consider the following impacts:

ASPECT	IMPACT DURING LHC MODE
Studio Access	Might be inaccessible, depending on the nature of the disruption. VDAs in zones operating in LHC mode displays as **Unregistered** in Studio because they are registered with the LHC broker.
Remote PowerShell SDK Access	Limited access. Set SDK Authentication: Run `Get-XDAuthentication -ProfileName WindowsCurrentUser` to prevent the SDK proxy from redirecting cmdlet calls. After making these changes, you can use all `Get-Broker` cmdlets. **Note**: Include the `-AdminAddress localhost:89` parameter in the initial cmdlet call. Example: `Get-BrokerMachine`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ASPECT	IMPACT DURING LHC MODE
	`-AdminAddress localhost:89`
Monitoring Data	Monitor functions don't show activity from when LHC mode is active. A subset of monitoring data is available in the Local Host Cache dashboard of the trends page in Monitor.
Hypervisor Credentials	Cannot be obtained from Host Service. Machines in an unknown power state, no power operations possible. Powered-on VMs usable for connections.
Assigned Machines	Usable only if assigned during normal operations. New assignments are impossible in LHC mode.
Remote PC Access Machines	Automatic enrollment and configuration not supported. Machines enrolled and configured during normal operation are usable.
Server-Hosted Application and Desktops Session Limits	Users might use more sessions than their configured session limits, if the resources are in different zones.
Zone Behavior	Each zone acts independently. If the StoreFront advanced health check feature is enabled, StoreFront is able to route launch requests to the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ASPECT	IMPACT DURING LHC MODE
	appropriate zone during LHC mode and avoid session launch failures.
Scheduled VDA Restarts	If LHC mode enters before a scheduled restart begins for VDAs in a delivery group, the restarts begin when LHC mode exits and normal brokering operations resume, potentially causing unexpected reboots when the zone leaves LHC mode. For more information and configurations that can alter this behavior, see Scheduled restarts delayed due to database outage.
Zone Preference	Zone preference configurations are not considered for session launch.
Tag Restrictions	For Delivery Groups with VDAs in multiple zones, tag restrictions can cause launch failures if tagged VDAs are not present in all zones.

NOTE:

The use of `$XDSDKAuth` for SDK authentication is deprecated starting June 2025. For details, see Deprecation.

Application and desktop support

LHC supports the following types of VDAs and delivery models:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA TYPE	DELIVERY MODEL	VDA AVAILABILITY DURING LHC MODE
Multi-session OS	Applications and desktops	Always available.
Single-session OS static (assigned)	Desktops	Always available.
Power-managed single-session OS random (pooled)	Desktops	Available for only one session by default. You can configure them to be always available for new sessions during LHC. For more information, see Enable using Studio and Enable using PowerShell. **Important:** Enabling access to power-managed single-session pooled machines can cause data and changes from previous user sessions being present in subsequent sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Enabling access to power-managed desktop VDAs in pooled delivery groups doesn't affect how the configured `ShutdownDesktopsAfterUse` property works during normal operations. When access to these desktops during LHC is enabled, VDAs don't automatically restart after returning to normal brokering operations. Power-managed desktop VDAs in pooled delivery groups can retain data from previous sessions until the VDAs restart. A VDA restart can occur when a user logs off the VDA during non-LHC operations or when administrators restart the VDA.

Enable LHC for power-managed single-session OS pooled VDAs using Studio

Using Studio, you can make those machines available for new connections during LHC mode on a per-delivery group basis:

- To enable this feature during delivery group creation, see Create delivery groups.
- To enable this feature for an existing delivery group, see Manage delivery groups

NOTE:

This setting is available in Studio only for pooled desktop delivery groups that deliver power-managed VDAs.

Enable LHC for power-managed single-session OS pooled VDAs using PowerShell

To enable LHC for VDAs in a specific delivery group, follow these steps:

1. Enable this feature at the site level by running this command:

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

2. Enable LHC for a delivery group by running this command with the delivery group name specified:

```
Set-BrokerDesktopGroup -Name "name"
-ReuseMachinesWithoutShutdownInOutage $true
```

To change the default LHC availability for newly created pooled delivery groups with power managed VDAs, run the following command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

NOTE:

Changing the default does not change the setting for existing Delivery Groups and only affects Delivery Groups created using PowerShell.

StoreFront configuration

If using an on-premises StoreFront deployment, review the following:

- If using a load balancing virtual server, configure the virtual server to monitor Connectors based on brokering capabilities (example, use the built-in CITRIX-XD-DDC monitor on a NetScaler® for connector load balancing).
- Include all Cloud Connectors within a single Cloud tenant as a single site in StoreFront.
- View NetScaler Gateway configurations in StoreFront and ensure that all Connectors are listed as STA servers. Review NetScaler appliances and ensure all STAs listed in StoreFront are in the same format in the NetScaler Gateway virtual server. STA service health can also be monitored in the Gateway virtual server.
- Add all connectors to the resource feed in StoreFront and ensure that StoreFront can communicate with all Cloud Connectors over the port designated in the resource feed.

NOTE:

For customers with many connectors, it may be beneficial to configure a load-balancing virtual server for each zone to reduce management overhead and simplify troubleshooting. See Citrix TIPs: Integrating Citrix Virtual Apps and Desktops service and StoreFront for more information.

Validate Local Host Cache working

To verify that LHC is set up and working correctly:

- Ensure that synchronization imports complete successfully. Check the event logs for more information on how to monitor LHC synchronizations.
- Ensure that the Local Host Cache database was created on each Cloud Connector. This confirms that the High Availability Service can take over, if needed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On the Cloud Connector server, browse to `c:\Windows\ServiceProfiles\NetworkService`.
- Verify that `HaDatabaseName.mdf` and `HaDatabaseName_log.ldf` are created.

- Force LHC mode on all Cloud Connectors in the zone: After you've verified that Local Host Cache works, remember to place all the Cloud Connectors back into normal mode. See Local Host Cache states for more information regarding the time it will take to leave LHC mode.

Monitor Local Host Cache

Event logs

Event logs provide critical information regarding the health and performance of LHC.

Config Synchronizer Service

During normal operations, the following events can occur when the CSS imports the configuration data into the LHC database using the LHC broker.

EVENT ID	DESCRIPTION
503	Indicates that the CSS received an updated configuration. This event occurs each time an updated configuration is received from Citrix Cloud. This indicates the start of the synchronization process.
504	Indicates that the CSS imported an updated configuration. The configuration import completed successfully.
505	Indicates that the CSS failed an import. The configuration import did not complete successfully. If a previous successful configuration is available, it is used if LHC mode is entered. However, it will be out-of-date from the current configuration. If there is no previous configuration available, the service cannot participate in session brokering during LHC mode. In this case, see the Troubleshoot section, and contact Citrix Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	DESCRIPTION
507	Indicates that the CSS abandoned an import because the system is in LHC mode and the LHC broker is being used for brokering. The service received a new configuration, but the import was abandoned because LHC mode was entered. This is expected behavior.
510	Indicates that no CSS configuration data received from primary Configuration Service.
517	Indicates that there was a problem communicating with the primary Broker Service.
518	Indicates that the CSS script aborted because the LHC broker (High Availability Service) is not running.

High Availability Service

This service is also known as the LHC broker.

EVENT ID	DESCRIPTION
3502	Indicates that an outage occurred and the LHC broker is performing broker operations.
3503	Indicates that an outage was resolved and normal operations have resumed.
3504	Indicates the LHC broker that is elected and other LHC brokers involved in the election.
3507	Indicates that LHC mode is active on the elected LHC broker. Contains a summary of the outage including outage duration, VDA registration, and session information.
3508	Indicates that LHC is no longer active on the elected LHC broker and normal operations have been restored. Contains a summary of the outage including outage duration, number

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT ID	DESCRIPTION
	of machines that registered during the LHC event, and number of successful launches during LHC mode.
3509	Indicates that LHC is active on the non-elected LHC broker. Contains an outage duration every 2 minutes and indicates the elected LHC broker.
3510	Indicates that the LHC is no longer active on the non-elected LHC broker. Contains the outage duration and indicates the elected LHC broker.

Remote Broker Provider

This service acts as a proxy between Citrix Cloud and your VDAs and Cloud Connectors.

EVENT ID	DESCRIPTION
3001	The first detection of a failure causing the Cloud Connector to enter the **Pending HA** state. Health checks start to assess whether the failure is a transient or persistent one. After the allotted time in **Pending HA** state, the latest health check results indicate whether an entry to LHC mode is required or if normal operations can be resumed.
3002	Indicates that the Cloud Connector cannot enter LHC mode. The reason is included in the event information.
3003	Indicates that the Cloud Connector is transitioning through LHC mode states.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

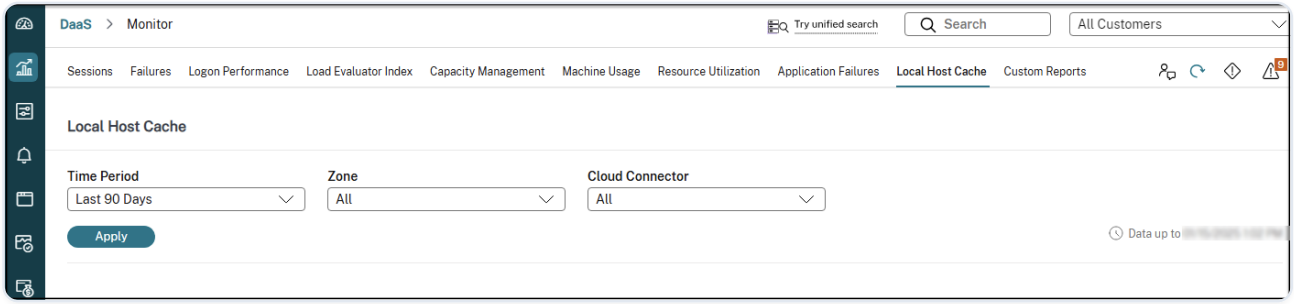
EVENT ID	DESCRIPTION	
	The event provides details about the following • state from which the Cloud Connector is transitioning • state to which it is transitioning • duration of the previous state	

NOTE:

The **3001** events on your Cloud Connectors periodically throughout the day are typically not a cause for concern. However, if they're occurring multiple times an hour, then it indicates a network issue and might warrant further investigation.

Citrix Monitor

Citrix Monitor contains centralized information regarding LHC mode entries and performance for the different Zones in your environment.



See Monitor historical trends across a site for more information.

Force Local Host Cache mode

You might want to deliberately force Local Host Cache mode in the following scenarios:

- If your network is going up and down repeatedly: Forcing LHC until the network issues are resolved prevents continuous transition between normal and LHC modes (and the resulting frequent VDA registration storms).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To test a disaster recovery plan.
- To help ensure that Local Host Cache is working correctly.

To force LHC mode:

1. Edit the registry of each Cloud Connector server in `HKLM\Software\Citrix\DesktopServer\LHC`: Create and set `OutageModeForced` as REG_DWORD to `1`.
    - Setting the value to `1` instructs the LHC broker to enter LHC mode, regardless of the state of the connection to Citrix Cloud.
    - Setting the value to `0` instructs the LHC broker to exit LHC mode and resume normal operations.

To verify events:

1. Monitor the `Current_HighAvailabilityService` log file in `C:\ProgramData\Citrix\workspaceCloud\Logs\Plugins\HighAvailabilityService`.

Troubleshoot synchronization import failures

When a synchronization import to the LHC database fails and a 505 event is logged, you can use the following troubleshooting tools:

- CDF Tracing:
    - Enable tracing for the `ConfigSyncServer` and `BrokerLHC` modules.
    - Use with other broker modules to identify the problem.
- CSS Trace Report:
    - Generates a detailed report that pinpoints the object causing the synchronization failure.

    NOTE:

    Enabling this report can impact synchronization speed. Disable it when not actively troubleshooting.

    To enable and generate a CSS Trace Report:

    a. Enable reporting: Run the following command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

b. Locate the report: The HTML report is generated at `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncRepo`

c. Disable reporting: After the report is generated, run the following command to disable the reporting feature:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

Local Host Cache PowerShell commands

You can manage Local Host Cache on your Cloud Connectors using PowerShell commands.

The PowerShell module is at the following location on the Cloud Connectors:

`C:\Program Files\Citrix\Broker\Service\ControlScripts`

IMPORTANT:

Run this module only on the Cloud Connectors.

Import PowerShell module

To import the module, run the following on your Cloud Connector:

```
Import-Module "C:\Program
Files\Citrix\Broker\Service\ControlScripts\HighAvailabilityServiceControl.
psm1
```

PowerShell commands to manage LHC

The following cmdlets help you to activate and manage the LHC mode on the Cloud Connectors.

CMDLETS	FUNCTION
`Enable-LhcForcedOutageMode`	Place the Broker in LHC mode. Local Host Cache database files must have been successfully created by the CSS for `Enable-LhcForcedOutageMode` to function properly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CMDLETS	FUNCTION
	This cmdlet only forces LHC on the Cloud Connector that it was run on. For LHC to become active, this cmdlet must be run on all Cloud Connectors within the zone.
`Disable-LhcForcedOutageMode`	Takes the Broker out of the LHC mode. This cmdlet only disables LHC mode on the Cloud Connector that it was run on. `Disable-LhcForcedOutageMode` must be run on all Cloud Connectors within the zone.
`Set-LhcConfigSyncIntervalOverride`	Sets the interval at which CSS checks for configuration changes within the Citrix DaaS™ site. The time interval can range from 60 seconds(one minute) to 3600 seconds(one hour). This setting only applies to the Cloud Connector on which it was run. For consistency across the Cloud Connectors, consider running this cmdlet on each Cloud Connector. For example: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Sets the interval at which the CSS checks for configuration changes within the Citrix DaaS site to the default value of 300 seconds (five minutes). This setting only applies to the Cloud Connector on which it was run. For consistency across the Cloud Connectors, consider running this cmdlet on each Cloud Connector.
`Enable-LhcHighAvailabilitySDK`	Enables access to all the `Get-Broker*` cmdlet within the Cloud Connector that it was run on.
`Disable-LhcHighAvailabilitySDK`	Disables access to the Broker PowerShell commands within the Cloud Connector that it was run on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Use port 89 when running the `Get-Broker*` cmdlets on the Cloud Connector. For example:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- When not in LHC mode, the LHC Broker on the Cloud Connector only holds configuration information.
- During LHC mode, the LHC Broker holds the following information:
  - Resource states
  - Session details
  - VDA registrations
  - Configuration information

More information

- See Scale and size considerations for Local Host Cache for information about:
  - Testing methodologies and results
  - RAM size considerations
  - CPU core and socket configuration considerations
  - Storage considerations
- Tech Brief: Local Host Cache
  - Avoid Common Misconfigurations that Can Negatively Impact DaaS Resiliency
- Local Host Cache (LHC) real-time visibility tool is a comprehensive PowerShell-based solution for providing visibility in Citrix Local Host Cache environments. It provides both command-line and simple GUI interfaces accessible from the Cloud Connector for you to:
  - Discover Cloud Connectors in a zone or resource location
  - Identify the elected leader during LHC mode
  - Enable or disable forced outage mode across all Cloud Connectors in the zone or resource location
  - Query event logs from specific providers and Event IDs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Run Broker PowerShell commands on the elected leader

For more information, see Local Host Cache Visibility Tool.

Local Host Cache Visibility Tool

This article describes the Local Host Cache (LHC) Real-time Visibility Tool, a PowerShell-based solution that provides visibility into Citrix Local Host Cache environments. Using this tool, you can monitor Cloud Connector health, identify the elected leader during LHC mode, control-forced outage mode, and query event logs to troubleshoot LHC behavior.

Overview

The Local Host Cache (LHC) Real-time Visibility Tool is a comprehensive PowerShell-based solution for providing visibility in Citrix Local Host Cache environments. It provides both a command-line interface and simple GUIs accessible from the Cloud Connector for you to:

- Discover Cloud Connectors in a zone or resource location.
- Identify the elected leader during LHC mode.
- Enable or disable forced outage mode across all Cloud Connectors in the zone or resource location.
- Query event logs from specific providers and Event IDs.
- Run Broker PowerShell commands on the elected leader.

Prerequisites

Before you deploy and run the Local Host Cache Visibility Tool, make sure that your environment meets the following system requirements, permissions, and file requirements.

System requirements

- Windows Server 2016 or later
- PowerShell 5.1 or higher
- Must be run on a Citrix Cloud Connector™
- Required services:
  - Citrix High Availability Service
  - Citrix ConfigSync Service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Permissions

- Administrator privileges on the local machine
- Remote PowerShell execution permissions for all Cloud Connectors in the zone
- Network connectivity to all Cloud Connectors

Files required

- `LHCVisibilityTool.ps1` - Core PowerShell module
- `LHCVisibilityToolGUI.ps1` - GUI application
- `HighAvailabilityServiceControl.psm1` - Citrix HA Service Control module

The GUI PowerShell script is located at:

```
C:\Program Files\Citrix\Broker\Service\LHCVisibilityToolScripts
```

Get started

Before you run the tool, set the PowerShell execution policy using one of the following options:

- Option 1: RemoteSigned (more restrictive):

  ```
  Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
  ```

- Option 2: Current session only (temporary):

  ```
  Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process
  ```

NOTE:

You might need to run PowerShell as Administrator to change the execution policy. If you have only user-level permissions, use `-Scope CurrentUser`.

Use the tool via the GUI application

The GUI provides a tabbed interface for discovering Cloud Connectors, controlling outage mode, querying event logs, and running broker commands. After you launch the tool, select a task to go to its instructions:

- Launch the GUI

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Discover Cloud Connectors and identify the leader
- Control forced outage mode
- Query and track event logs
- Run broker commands
- View session logs

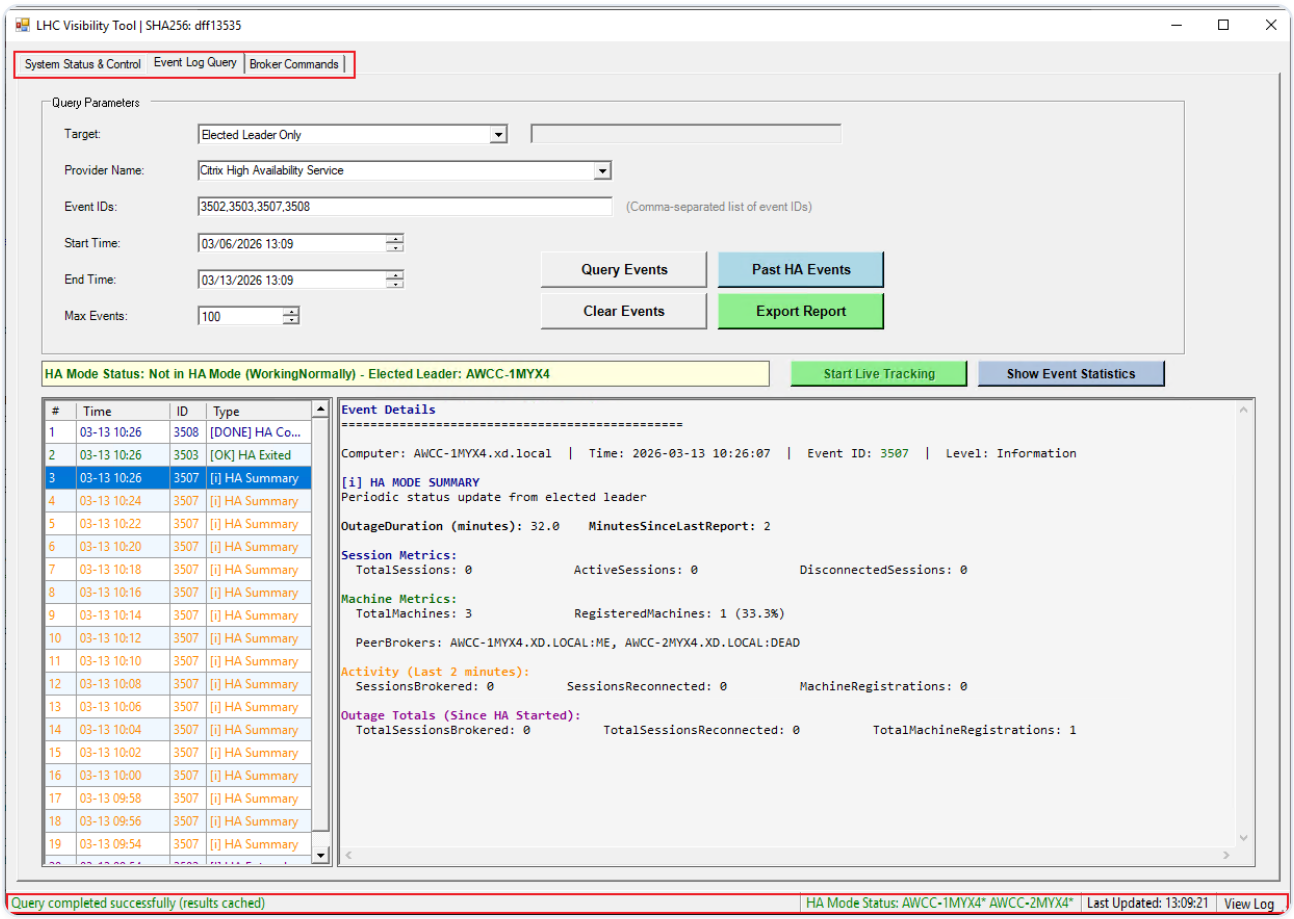
LAUNCH THE GUI

```
cd "C:\Program Files\Citrix\Broker\Service\LHCVisibilityToolScripts"

.\LHCVisibilityToolGUI.ps1
```

```
PS C:\Program Files\Citrix\Broker\Service> cd "C:\Program Files\Citrix\Broker\Service\LHCVisibilityToolScripts"
PS C:\Program Files\Citrix\Broker\Service\LHCVisibilityToolScripts> .\LHCVisibilityToolGUI.ps1
```

The tool uses a three-tab layout with a persistent status bar at the bottom.



The status bar spans the bottom of the window and contains:

ITEM	DESCRIPTION
Operation status (left)	Current operation, or "Ready"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DESCRIPTION
HA Mode Status	Per-connector dot indicators (maximum 5 shown; "+N more" if truncated); the hover tooltip shows the full list
Last Updated	Timestamp of the last successful HA state refresh
View Log	Opens the session log file in Notepad

The status bar uses the following colors to indicate the HA state:

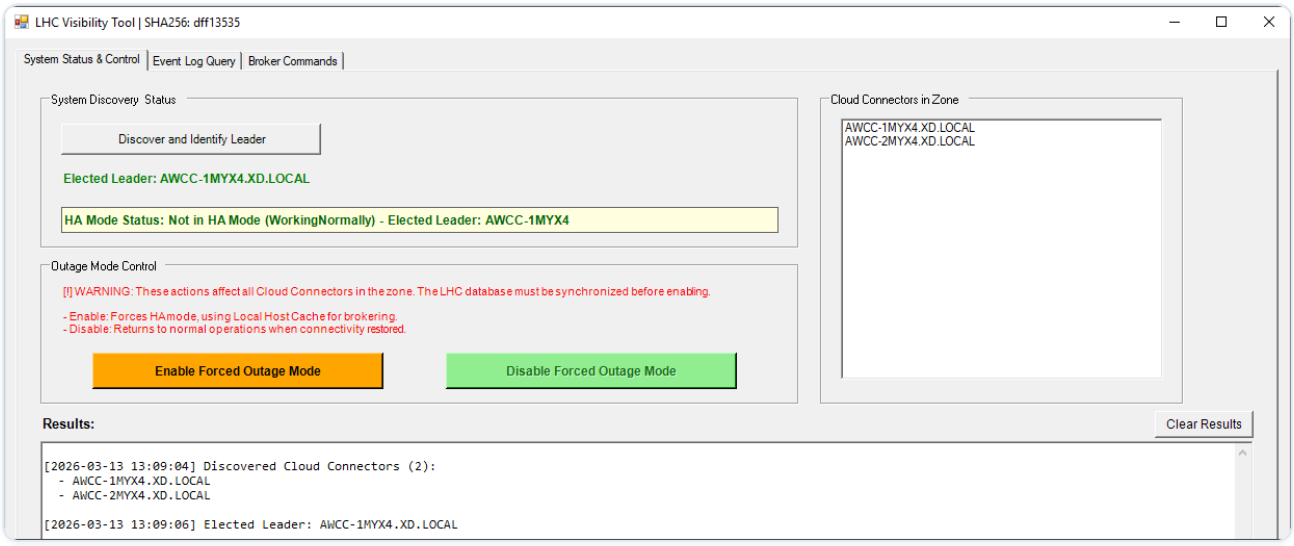
STATE	COLOR
WorkingNormally	Green
PendingHA	Goldenrod
PendingRecovery	Orange
InitialHA	Red
ExtendedHA	Red
Unknown / Unreachable	Gray

DISCOVER CLOUD CONNECTORS AND IDENTIFY THE LEADER

On the **System Status & Control** tab, click **Discover and Identify Leader**. The tool automatically detects and shows the elected leader among all Cloud Connectors in the zone using:

- Event log analysis (Event ID 3504)
- Registry PeerStatus and IsElected information
- Local service verification

© 1997–2026 Citrix Systems, Inc. All rights reserved.



CONTROL FORCED OUTAGE MODE

On the **System Status & Control** tab, use the outage mode controls to manage HA mode across the zone:

- **Enable Forced Outage Mode:**
  - Forces all Cloud Connectors in the zone to enter HA mode
  - Uses Local Host Cache for brokering
  - Requires the LHC database to be synchronized
- **Disable Forced Outage Mode:**
  - Allows the system to return to normal operations
  - Reconnects to the primary site when available

WARNING:

These actions affect all Cloud Connectors in the zone.

QUERY AND TRACK EVENT LOGS

On the **Event Log Query** tab, configure the following query parameters:

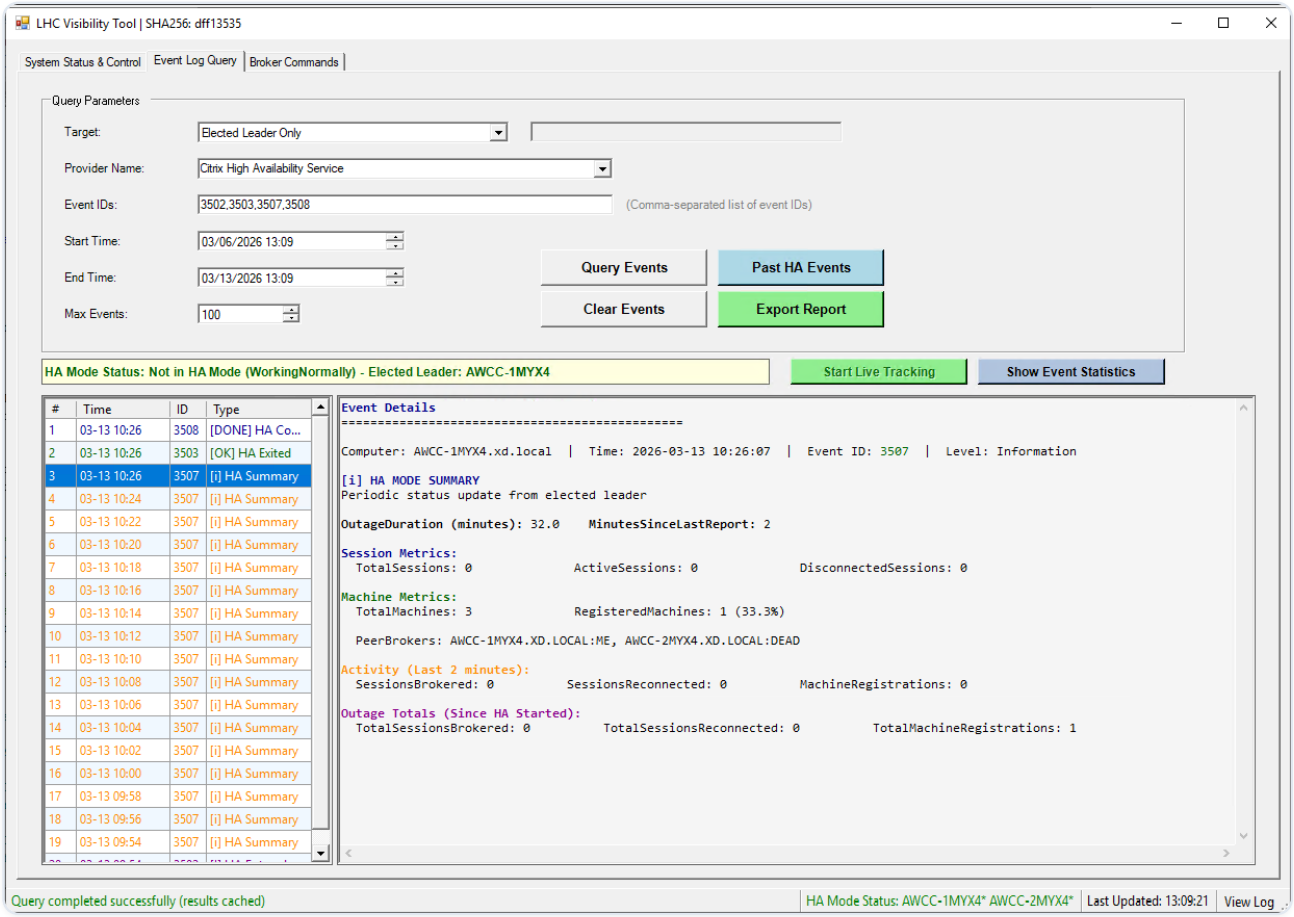
- **Target:** Choose from:
  - All Cloud Connectors
  - Elected Leader Only
  - Specific Computer (enter FQDN)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Provider Name:** Select or enter a custom provider:
  - Citrix High Availability Service
  - Citrix ConfigSync Service
  - Citrix Broker Service
- **Event IDs:** Comma-separated list (for example, `3502,3503,3506`)
- **Time Range:** Optionally filter by start and end time
- **Max Events:** Maximum number of events to retrieve per computer (default: 100)

Use the following buttons to work with events:

- **Query Events:** Queries the event logs using the configured query parameters.
- **Past HA Events:** Finds LHC begin and end boundaries (events 3502, 3503, 3508) from the configured query parameters and display the end summary event to give an overview.
- **Clear Events:** Clears the event list, detail panel, and tracking state.
- **Export Report:** Creates statistics from the queried events in the GUI and saves them as a text file. (Uses the output from the **Show Event Statistics** button.)



Live tracking behaves as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

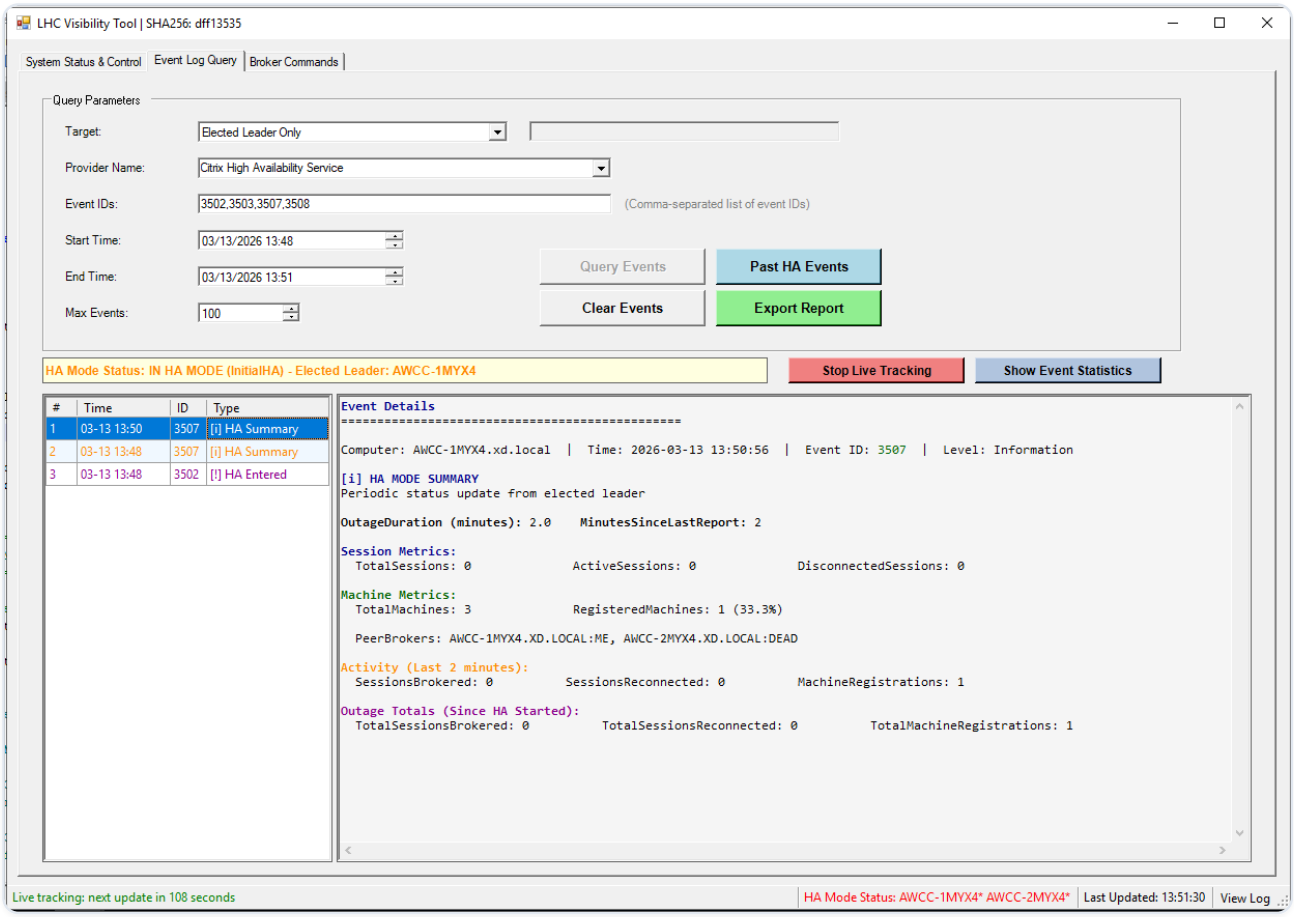
- Live tracking monitors for new summary events every 120 seconds while LHC is active.
- When live tracking begins, it determines the start time for LHC mode by referencing event 3502 and lists all events that appeared since the start.
- Live tracking can be stopped manually, or automatically when LHC mode concludes.

The lower section provides two main views:

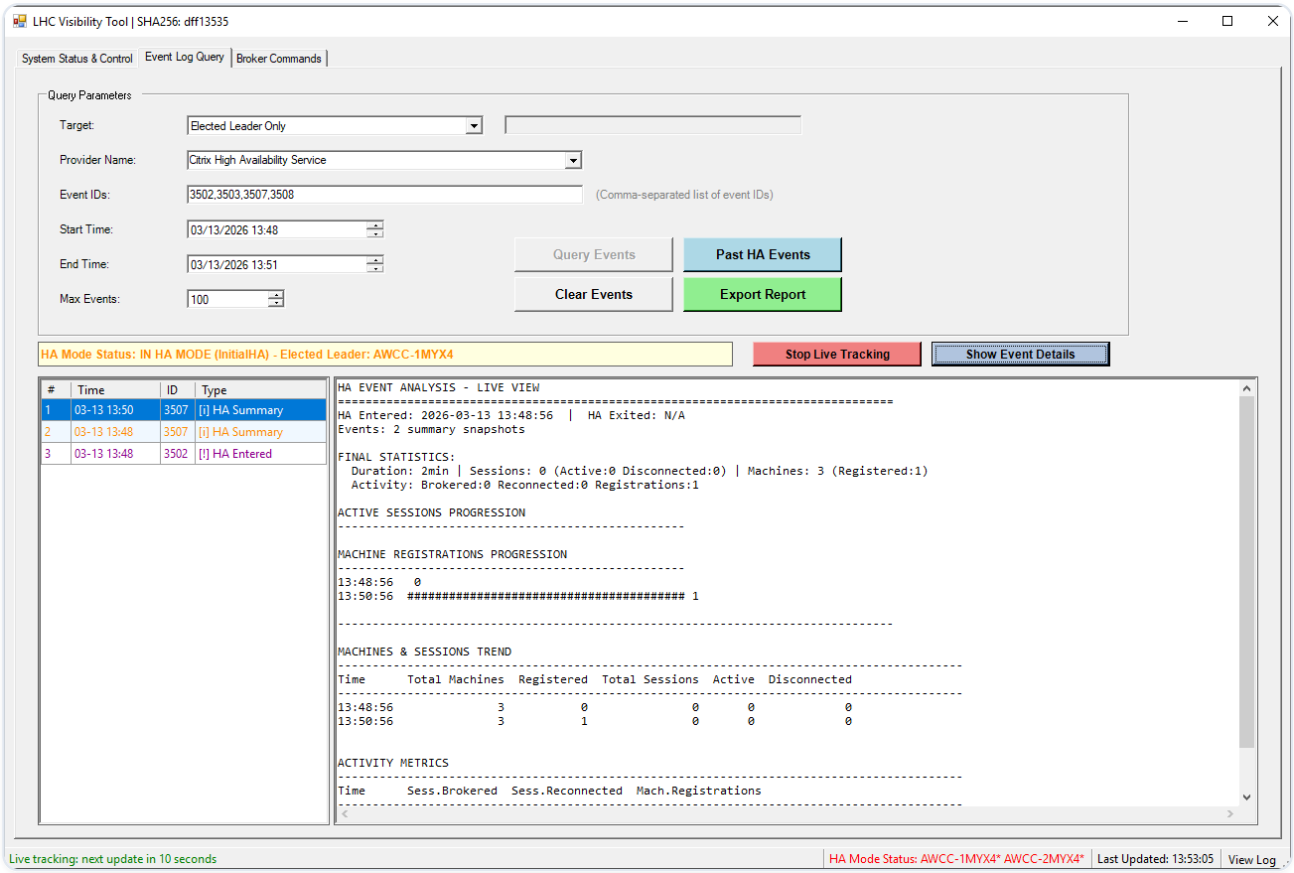
- **Left panel:**
  - Events are listed chronologically with key details (event number, time, ID, type).
  - Each event is visually distinguished by color based on its type, following the event ID reference.
  - Selecting an event displays further information about it.
- **Right panel:** Two display options let you toggle between statistical summaries and detailed information for the selected event:
  - **Show Event Details:** Comprehensive details for the chosen event.
  - **Show Event Statistics:** Statistics summarizing HA mode events, including tabular metrics and ASCII bar charts from summary events (3507).

The following image shows the event details view:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following image shows the event statistics view:



Reference: HA and ConfigSync event IDs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following sections list common Event IDs by provider.

Citrix High Availability Service:

EVENT ID	DESCRIPTION
3502	HA mode entered (elected broker)
3503	Out of HA mode (normal operations resumed)
3506	HA mode entered (non-elected broker)
3507	Periodic HA mode summary (elected broker)
3508	End of HA mode summary (elected broker)

Citrix ConfigSync Service:

EVENT ID	DESCRIPTION
503	Synchronization process started
504	Synchronization completed successfully
505	Synchronization failed
507	Sync abandoned due to HA mode
510	No configuration data received
517	Problem communicating with primary broker
518	ConfigSync aborted (HA Service not running)

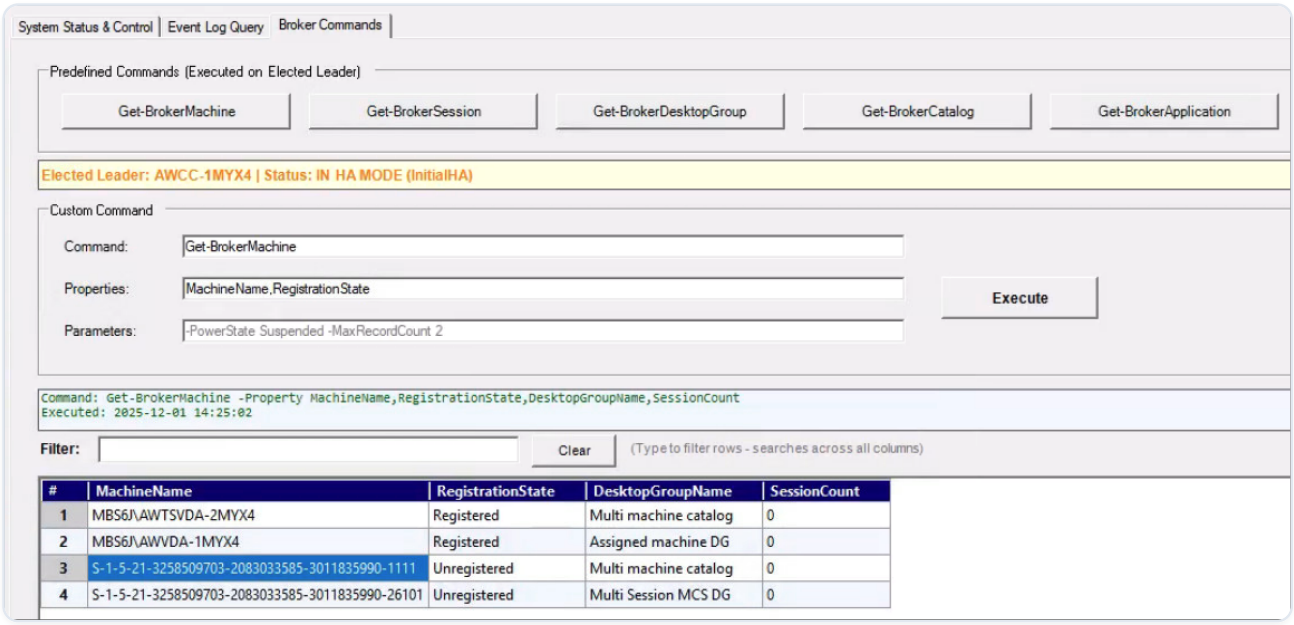
RUN BROKER COMMANDS

On the **Broker Commands** tab, the predefined commands are:

- **Get-BrokerMachine:** Retrieve VDA/machine information
- **Get-BrokerSession:** Retrieve active sessions
- **Get-BrokerDesktopGroup:** Retrieve delivery groups
- **Get-BrokerCatalog:** Retrieve machine catalogs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Get-BrokerApplication:** Retrieve published applications

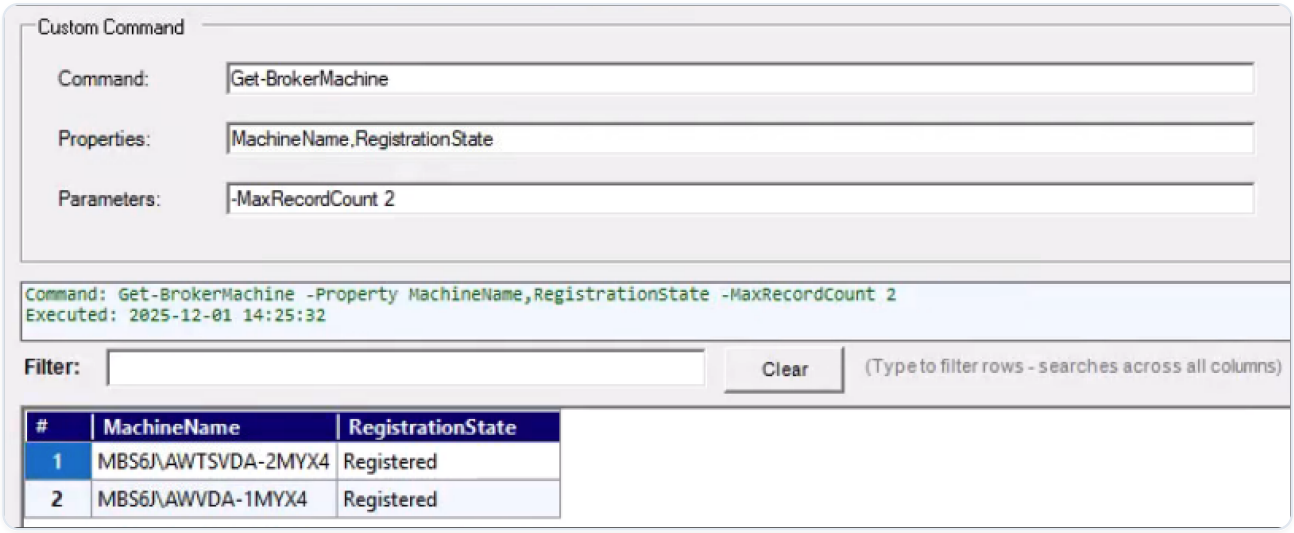


TIP:

Use the filter text box to search across all string columns simultaneously for a specific item in the results.

To run a custom command:

1. Enter a command, for example `Get-BrokerMachine -MaxRecordCount 2`.
2. Optionally specify the properties to return (comma-separated).
3. Click **Execute**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Broker commands give recent information from the LHC database when:

- The system is in LHC mode.
- An elected leader has been identified.
- The LHC database is available.

VIEW SESSION LOGS

To open the current session log, click **View Log** in the status bar. The log opens in Notepad.

Each session creates a log file at `%TEMP%\LHCVisibilityTool_<yyyyMMdd_HHmmss>.log`. Messages are also written to the host console with color coding.

Use the tool via the command line

In addition to the GUI, you can run the tool directly from PowerShell. After you import the module, use the following commands to perform each task. Select a task to go to its command:

- Launch the command-line tool
- Discover Cloud Connectors
- Identify the elected leader
- Get the outage state
- Query event logs
- Run broker commands
- Control outage mode

LAUNCH THE COMMAND-LINE TOOL

```
cd "C:\Program Files\Citrix\Broker\Service\LHCVisibilityToolScripts"

. .\LHCVisibilityTool.ps1
```

DISCOVER CLOUD CONNECTORS

```
$connectors = Get-CloudConnectorsInZone

$connectors | ForEach-Object { Write-Host $_ }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IDENTIFY THE ELECTED LEADER

```
$leader = Get-ElectedLeader

Write-Host "Elected Leader: $leader"
```

GET THE OUTAGE STATE

```
$states = Get-OutageState

foreach ($connector in $states.Keys) {

    Write-Host "$connector : $($states[$connector].State)"

}
```

QUERY EVENT LOGS

Query all Cloud Connectors for HA events:

```
$results = Get-LHCEventLogs -EventID @(3502, 3503, 3506) `

    -ProviderName "Citrix High Availability Service" `

    -StartTime (Get-Date).AddDays(-7) `

    -EndTime (Get-Date) `

    -MaxEvents 100



# Display results

foreach ($computer in $results.Keys) {

    Write-Host "`n=== $computer ==="

    if ($results[$computer].Success) {

        $results[$computer].Events | Format-Table TimeCreated, Id, Message
-AutoSize

    } else {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        Write-Host "ERROR: $($results[$computer].Error)" -ForegroundColor
Red

    }

}
```

Query only the elected leader:

```
$results = Get-LHCEventLogs -ComputerName "ElectedLeader" `

    -EventID @(3507) `

    -ProviderName "Citrix High Availability Service" `

    -MaxEvents 50
```

Query a specific computer:

```
$results = Get-LHCEventLogs -ComputerName "CC-01.domain.com" `

    -EventID @(503, 504, 505) `

    -ProviderName "Citrix ConfigSync Service"
```

RUN BROKER COMMANDS

Get all machines:

```
$machines = Invoke-BrokerCommand -Command "Get-BrokerMachine" `

    -Properties @("MachineName", "RegistrationState", "SessionCount")

$machines | Format-Table -AutoSize
```

Get active sessions:

```
$sessions = Invoke-BrokerCommand -Command "Get-BrokerSession" `

    -Properties @("UserName", "MachineName", "SessionState")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$sessions | Format-Table -AutoSize
```

Run a custom command with parameters:

```
$params = @{

    MaxRecordCount = 10

}

$results = Invoke-BrokerCommand -Command "Get-BrokerMachine" `

    -Parameters $params `

    -Properties @("MachineName", "DesktopGroupName")
```

CONTROL OUTAGE MODE

Enable forced outage mode on all Cloud Connectors:

```
$results = Set-LHCOutageMode -Enable



# Check results

foreach ($connector in $results.Keys) {

    $status = if ($results[$connector].Success) { "SUCCESS" } else
{ "FAILED" }

    Write-Host "$connector : $status"

    if (-not $results[$connector].Success) {

        Write-Host "  Error: $($results[$connector].Error)"
-ForegroundColor Red

    }

}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Disable forced outage mode:

```
$results = Set-LHCOutageMode



# Check results

foreach ($connector in $results.Keys) {

    $status = if ($results[$connector].Success) { "SUCCESS" } else
{ "FAILED" }

    Write-Host "$connector : $status"

}
```

Troubleshooting

To troubleshoot issues with the tool, follow this general process:

1. Check the Application event log for detailed error messages.
2. Verify that all prerequisites are met.
3. Review the common issues in the following table and the best practices described later in this article.
4. Refer to Local Host Cache and the Avoid Common Misconfigurations that Can Negatively Impact DaaS Resiliency technical brief.

The following table lists common issues that you might encounter when using the tool and their recommended solutions.

ISSUE	SOLUTION
No Cloud Connectors found	1. Verify that you're running on a Cloud Connector. 2. Check that the required services are running by using `Get-Service CitrixHighAvailabili`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE	SOLUTION
	`tyService, CitrixConfigSyncService`. 3. Check the registry key `HKLM:\SOFTWARE\Citrix\Broker\Service\State\LHC`.
Cannot identify elected leader	1. Check for Event ID 3502 in the Application log. 2. Verify connectivity to all Cloud Connectors.
Broker command failed	1. Ensure that the system is in HA mode. 2. Verify that the elected leader is identified. 3. Check that the LHC database is synchronized. 4. Verify that `HighAvailabilityServiceControl.psm1` is present.
Remote execution errors	1. Verify that WinRM is enabled on all Cloud Connectors by using `Test-WSMan -ComputerName`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE	SOLUTION	
	`<CloudConnectorFQDN>`. 2. Check that firewall rules allow PowerShell remoting. 3. Verify that you have administrator privileges.	
Event log query returns no results	1. Verify that the Event IDs are correct for the selected provider. 2. Check that the time range encompasses the expected events. 3. Ensure that event log size limits haven't caused old events to be overwritten.	

Best practices

Follow these best practices to get the most out of the tool and to operate your Local Host Cache environment safely.

Regular monitoring

- Run **Discover Cloud Connectors** and **Identify Elected Leader** periodically.
- Monitor `ConfigSync` events (503, 504, 505) for synchronization issues.

Event log analysis

- Query the last 7 days of HA events to understand outage patterns.
- Look for Event ID 3507 during HA mode for detailed statistics.

Broker commands

- Only run on the elected leader.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Limit property selection to improve performance.
- Use the `MaxRecordCount` parameter for large environments.

Outage mode

- Only use forced outage mode for testing or planned maintenance.
- Always verify that the LHC database is synchronized before enabling.
- Disable forced outage mode once primary connectivity is restored.

Security

- Run with tleast-privilege accounts where possible.
- Use secure channels for remote execution.
- Audit outage mode changes.

Examples

The following examples assume that you have created a folder at `C:\Reports` to hold the output.

Example 1: Daily HA mode report

```
# Import module

. "C:\Program
Files\Citrix\Broker\Service\LHCVisibilityToolScripts\LHCVisibilityTool.ps1
"



# Discover environment

$connectors = Get-CloudConnectorsInZone

Write-Host "Found $($connectors.Count) Cloud Connectors"



# Check HA status

$leader = Get-ElectedLeader

if ($leader) {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    Write-Host "System is in HA mode. Elected leader: $leader"



    # Get HA summary events from elected leader

    $events = Get-LHCEventLogs -ComputerName "ElectedLeader" `

        -EventID @(3507, 3508) `

        -ProviderName "Citrix High Availability Service" `

        -StartTime (Get-Date).AddHours(-24) `

        -MaxEvents 100



    # Export to file

    $events[$leader].Events | Select-Object TimeCreated, Id,
LevelDisplayName, Message | Export-Csv -Path "C:\Reports\HA-Status-$(Get-
Date -Format 'yyyyMMdd').csv" -NoTypeInformation

} else {

    Write-Host "System is in normal operations mode"

}
```

Example 2: Check ConfigSync status on all connectors

```
. "C:\Program
Files\Citrix\Broker\Service\LHCVisibilityToolScripts\LHCVisibilityTool.ps1
"



$results = Get-LHCEventLogs -ComputerName "All" `

    -EventID @(503, 504, 505) `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    -ProviderName "Citrix ConfigSync Service" `

    -StartTime (Get-Date).AddHours(-6) `

    -MaxEvents 10



foreach ($computer in $results.Keys) {

    $lastEvent = $results[$computer].Events | Sort-Object TimeCreated
-Descending | Select-Object -First 1

    $status = switch ($lastEvent.Id) {

        503 { "In Progress" }

        504 { "Success" }

        505 { "Failed" }

    }

    Write-Host "$computer - Last Sync: $($lastEvent.TimeCreated) - Status:
$status"

}
```

Example 3: Get session count during HA mode

```
. "C:\Program
Files\Citrix\Broker\Service\LHCVisibilityToolScripts\LHCVisibilityTool.ps1
"



# Ensure we have an elected leader

$leader = Get-ElectedLeader

if ($leader) {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    # Get all sessions
    $sessions = Invoke-BrokerCommand -Command "Get-BrokerSession"
    Write-Host "Total Sessions: $($sessions.Count)"

    # Group by state
    $sessionsByState = $sessions | Group-Object SessionState
    foreach ($group in $sessionsByState) {
        Write-Host "  $($group.Name): $($group.Count)"
    }
} else {
    Write-Host "Not in HA mode - cannot query sessions from LHC"
}
```

Advanced scenarios

The following scenarios combine multiple tool functions into scripts for more complex operations, such as automating outage testing and exporting historical HA mode data.

Automate outage testing

```
# Enable outage mode
Write-Host "Enabling forced outage mode..."
$enableResults = Set-LHCOutageMode -Enable
$allEnabled = $enableResults.Values | Where-Object { -not $_.Success }
if ($allEnabled) {
    Write-Host "WARNING: Some connectors failed to enable outage mode -
aborting test" -ForegroundColor Yellow
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    return
}
Start-Sleep -Seconds 30


# Verify elected leader
$leader = Get-ElectedLeader
Write-Host "Elected leader: $leader"


# Test brokering
$machines = Invoke-BrokerCommand -Command "Get-BrokerMachine" -Properties
@("MachineName", "RegistrationState")
Write-Host "Retrieved $($machines.Count) machines"


# Disable outage mode
Write-Host "Disabling forced outage mode..."
$disableResults = Set-LHCOutageMode
```

Export HA mode history

```
$haEvents = Get-LHCEventLogs -ComputerName "All" `
    -EventID @(3502, 3503) `
    -ProviderName "Citrix High Availability Service" `
    -StartTime (Get-Date).AddDays(-30) `
    -MaxEvents 1000
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$report = foreach ($computer in $haEvents.Keys) {

    if (-not $haEvents[$computer].Success) { continue }

    foreach ($event in $haEvents[$computer].Events) {

        [PSCustomObject]@{

            Computer  = $computer

            EventID   = $event.Id

            EventType = if ($event.Id -eq 3502) { "Entered HA Mode" } else
{ "Exited HA Mode" }

            Time      = $event.TimeCreated

        }

    }

}

$report | Sort-Object Time | Export-Csv -Path "C:\Reports\HA-History.csv"
-NoTypeInformation
```

Log server settings

Configure log server settings, including the server address, port, and logging scope. **Monitor** uses these settings to connect to the log server and retrieve logs for monitoring and troubleshooting.

To complete this task, follow these steps:

1. Sign in to **Web Studio** and select **Settings** in the left pane.
2. If no log server is configured, click **Add** in the **Log server** tile.
3. On the **Log server** page, enter **Log server address** and **Port**.
4. To define which VDAs forward logs to the log server, follow these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Select **Select delivery groups**. By default, **All delivery groups** is selected, which forwards logs on VDAs in all delivery groups to the log server.

b. To forward logs only on VDAs in specific delivery groups, select **Select specific delivery groups**, and then choose the groups you want to include.

5. Select the **zone** where the log server resides.
6. Enter the **Authkey** generated by the log server. **Monitor** uses this key to authenticate and retrieve logs from the server.
7. Click **Save** to apply the configuration. To update the log server or modify the logging scope, click **Edit** in the **Settings > Log server** tile.

Machines and sessions (Search > Default view)

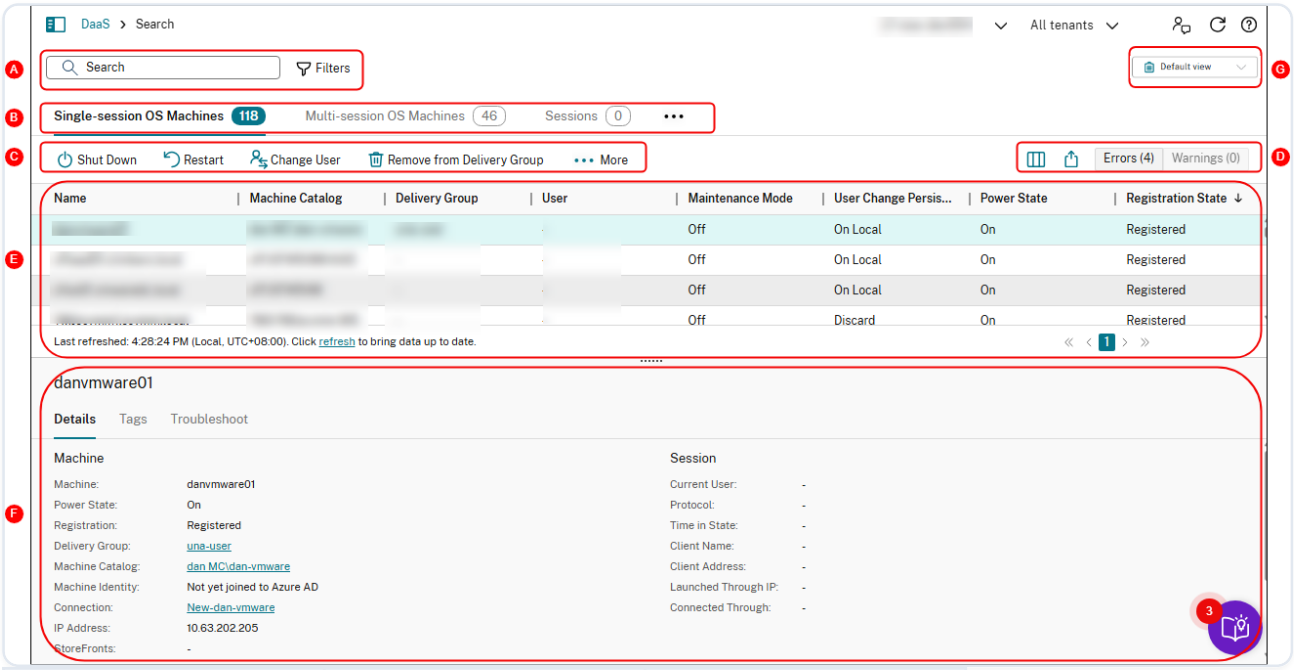
This article guides you through how to monitor and manage machines and sessions using Default view within the **Search** node. It contains the following topics:

- Learn about Default view
- Search for machines and sessions
- Customize cloumns to display
- Manage machines and sessions
- Export machine or session data to CSV files

Learn about the default view

The defaut view within the **Search** node provides a central place for monitoring and managing machines and user sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



CALLOUT	AREA	DESCRIPTION
A	Search bar	Provides a quick search and a filter-based search that allows you to define complex search criteria. For more information, see Search for instances.
B	Type tabs	Displays tabs to list machines by type or list all sessions. Instance counts appear in the tab names.
C	Instance-level actions	Displays actions that you can perform on the selected *instances* (machines or sessions). For more information, see Machine actions and Session actions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CALLOUT	AREA	DESCRIPTION
D	List-level actions	Displays actions that you can perform on the current *list*: • **Export** icon: Export the list of instances displayed in the main view to a CSV file. • **Column to display** icon: Customize the main view for the list. • **Errors** label: Enable this label to display only unregistered machines with errors in the main view. To view issue details, go to the **Troubleshoot** tab in the **Details** pane. • **Warning** label: Enable this label to display only unregistered machines with warnings in the main view. To

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CALLOUT	AREA	DESCRIPTION
		view issue details, go to the **Troubleshoot** tab in the **Details** pane.
E	Main view	Displays the instances and their properties. You can customize the main view by selecting the **Column to display** icon. For more information about available columns, see Machine columns and Session columns.
F	Details pane	Displays the following details: • Details of the selected instance (machine or session) • Tags applied to the selected machine • Details of errors or warnings with the selected machine, including problems, possible

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CALLOUT	AREA	DESCRIPTION
		causes, and suggested solutions
G	Switch to Hardware view	Click to switch from Default view to Hardware view.

Search for instances

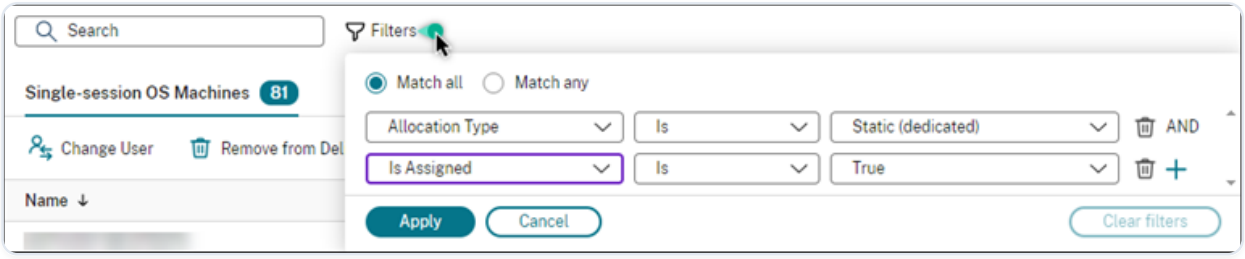
Use the search function to locate specific machines and sessions:

- Search using filters
- Save the current filter set for a quick search
- Pin a filter field in the search bar
- Search using the quick search box
- Tips to enhance a search

Search using filters

For example, to locate all single-session OS machines that are *static* and *assigned to users*, follow these steps:

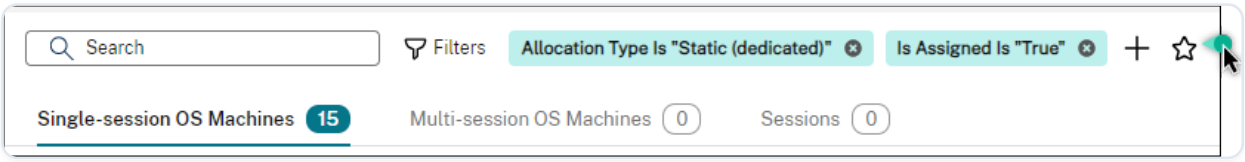
1. On the **Single-session OS machines** tab, click the **Filters** icon. The Filters panel appears.
2. Add the necessary filter criteria.



3. Select **Match all** (AND operator) if you want the search to return results that match all filter criteria. Select **Match any** (OR operator) if you want the search to return results that match any of the filter criteria.
4. Click **Apply**.

   The filtered list displays all single-session OS machines that are static and assigned to users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

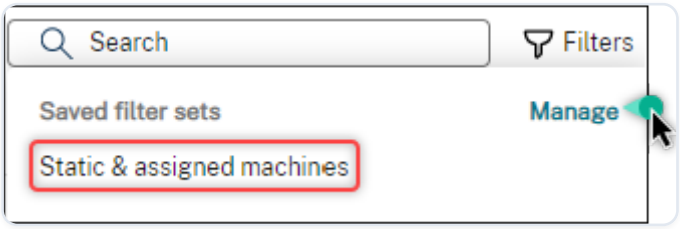


Save the current filter set for a quick search

For example, to save the filter set for single-session OS machines that are static and assigned to users for future use, follow these steps:

1. After you conduct a filter-based search, click the **Star** icon in the search bar, as shown in the preceding figure.
2. On the page that appears, enter a name for this filter set (for example, *Static & assigned machines*).
3. Click **Save**.

   The saved filter set appears in the search history list when you click the search box.



NOTE:

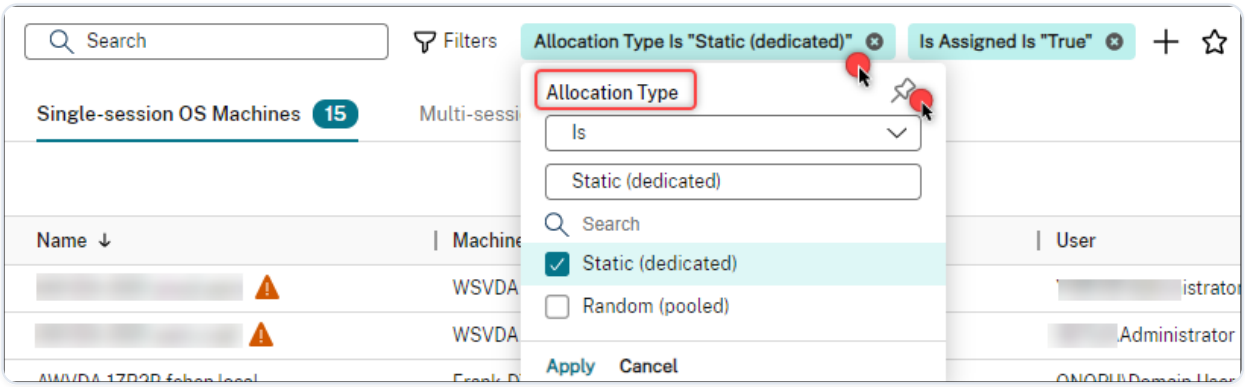
Filter sets are saved on a per user account basis. To manage saved filter sets, select **Manage**.

Pin a filter field in the search bar

Pin frequently used filter *fields* in the search bar for easy access. For example, after conducting a filter-based search, you want to pin **Allocate Type** in the search bar. Follow these steps:

1. Click the *filter setting* in the search bar.
2. In the panel that appears, click the **Pin** icon to pin the filter field (*Allocation Type* for this example) in the search bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Search using the quick search box

The quick search box provides a convenient way to search for instances based on name-related properties or saved filter sets. Detailed steps are as follows:

1. Click the search box. Your recent searches and saved filter sets appear in the drop-down list. You can click a previous search or filter set for a quick search.
2. To start a new search, enter a complete or partial name from the following options:
   - Machine name or DNS name
   - Machine catalog name
   - Delivery group name
   - Session user name
   - Session client name
   - Friendly name of the VM hosting the session, as used by its hypervisor
   - Hosting server name

Tips to enhance a search

Consider the following tips when using the Search feature:

- On the **Search** node, select any column to sort items.
- To show more characteristics to include in the display where you can search and sort, select **Columns to Display** or click any column and select **Columns to Display**. In the **Columns to Display** window, select the checkbox next to the items you want to display and select **Save** to exit.

> **NOTE:**
>
> Columns that degrade performance are marked with the **Degrades performance** label.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To locate a user device connected to a machine, use **Client (IP)** and **Is**, and enter the device IP address.
- To locate active sessions, use **Session State**, **Is**, and **Connected**.
- To list all machines in a delivery group, select **Delivery Groups** in the left pane. Select the group, and then select **View Machines** from the action bar or the context menu.
- To quickly narrow down MCS-provisioned machines by specific properties, use the **Search** bar available in Hardware view.

Keep the following considerations in mind when performing sorting operations:

- As long as the number of items does not exceed 5,000, you can click any column to sort the items in it. When the number exceeds 5,000, you can sort only by name or by current user (depending on which tab you are on). To enable sorting, use filters to reduce the number of items to 5,000 or fewer.
- When the number of items is greater than 500 but no more than 5,000:
  - We cache all data locally to improve sort performance. On the **Single-session OS Machines** and **Multi-session OS Machines** tabs, we cache the data the first time you click a column (any column except the **Name** column) to sort. On the **Sessions** tab, we cache the data the first time you click a column (any column except the **Current User** column) to sort. As a result, the sort takes longer to complete. For faster performance, sort by name or current user, or use filters to reduce the number of items.
  - The following message under the table indicates that the data is cached: Last refreshed: `<the time when you refreshed the table>`. In that case, sort operations are based on items that were loaded previously. Those items might not be up to date. To bring them up to date, click the refresh icon.

Customize columns to display

Create a personalized main view to display the properties and statuses crucial for your daily operations. Detailed steps are as follows:

1. In the **Search** node, select the **Multi-session OS Machines**, **Single-session OS Machines**, or **Sessions** tab as necessary.
2. Click the **Columns to display** icon in the action bar and select the columns.

   For more information about the available columns and their descriptions, see Machine columns and Session columns.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When choosing columns, you can see columns marked with the **Degrades performance** label. Selecting those columns might degrade the performance of the console. Keep these considerations in mind:

- After you complete your customization, the table refreshes to display the columns you select. Their presence might result in delays when you refresh the table.
- After you refresh the browser or sign out of the console and then sign in, a message appears asking whether to preserve those columns. If you choose to preserve them, you're restricted to refreshing the table more than once a minute for optimal console performance. For more frequent refreshes, remove any columns that degrade performance.

Manage machines and sessions

Use actions in the Search node to troubleshoot machines and session issues or process user requests.

Good to know

You can manage machines at different levels:

- At the individual machine level. Use the **Search** node to locate target machines and perform actions.
- At the machine catalog level, such as changing master images for a catalog, deleting machines from a catalog, and adding machines to a catalog. For more information, see Manage machine catalogs.
- At the delivery group level, such as turning on or off maintenance mode for machines in a group. For more information, see Manage delivery groups.

In addition to the individual session level, You can also manage sessions at the delivery group level, such as configuring session prelaunch and linger for a delivery group. For more information, see Manage Delivery Groups.

Perform actions on machines or sessions

To manage machines or sessions at the individual instance level, follow these steps:

1. In the **Search** node, select the **Multi-session OS Machines**, **Single-session OS Machines**, or **Sessions** tab.
2. Select one or more instances as necessary.
3. From the action bar or right-click menu, select an action based on the issues that you encounter with those instances or user requests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about the available actions and their descriptions, see Machine actions and Session actions.

NOTE:

If you select two or more instances, only actions that apply to all of them are available.

Export machine or session data to CSV files

Export the list of instances (machines or sessions) displayed on a tab (up to 30,000 items) to a CSV file. Detailed steps are as follows:

1. In the **Search** node, select the **Multi-session OS Machines**, **Single-session OS Machines**, or **Sessions** tab as necessary.
2. Click the **Export** icon in the upper right corner.
3. In the dialog box that appears, click **Continue**.

   The export might take several minutes to complete. You can find the file in the default download folder of your browser.

NOTE:

On each tab of the **Search** node, you cannot perform another export while an export is in progress.

Machine actions and columns

This article lists machine actions, machine columns, and their descriptions.

Actions

View the actions you can perform on machines and their descriptions. Some actions support the **Select all** operation, allowing you to apply the action to all machines across all pages.

ACTION	DESCRIPTION	APPLIES TO
Run Health Check	Available only for registered Windows VDAs, version 2019 or later. Run a health check on a machine.	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	APPLIES TO
	For more information about the checking contents, see About health checks.	
Remove from Delivery Group	Remove a machine from the delivery group.	Single-session and multi-session
Add to Delivery Group	Add a machine to a delivery group.	Single-session and multi-session
View Sessions	View the sessions running on a machine	Single-session and multi-session
Manage Tags	Add and manage tags for a machine. For more information about typical use cases of tags, see Tags.	Single-session and multi-session
Turn On Maintenance Mode	Place a machine in maintenance mode before applying patches, or for troubleshooting.	Single-session and multi-session
	This mode prevents new connections from being made to that machine. Users can connect to existing sessions on that machine, but they can't start new sessions on that machine.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	APPLIES TO
Turn Off Maintenance Mode	Turn off maintenance mode for a machine.	Single-session and multi-session
Upgrade VDA	Upgrade VDA for a machine.	Single- or multi-session OS machines that meet certain requirements: Learn more.
Log Off	Force log off a machine	Single-session and multi-session
Delete	Delete a VM from a machine catalog while leaving it intact on the hypervisor or cloud service.	Single-session and multi-session
Change User	Assign a machine to a specific user.	single-session *static* machines.
Start	Start a machine.	Single-session and multi-session
Shut Down	Shut down a machine.	Single-session and multi-session
Restart	Restart a machine	Single-session and multi-session
Suspend	Place a machine in a hibernation or suspension state. When you suspend a machine, DaaS stores the memory contents of the machine in a file and then shuts down the machine.	Single-session OS machines

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	APPLIES TO
Resume	Resume a suspended machine. When you resume a suspended machine, the DaaS starts the machine and restores it to the previous state.	Single-session OS machines
Force Restart	Force restart a machine.	Single-session OS machines
Force Shut Down	Force shut down a machine.	Single-session OS machines
View in Monitor	Open the detailed view of a machine in Monitor. This action is available only to roles with the **Director > Manage > View Machine Details** page permission.	Single-session and multi-session OS machines

Columns

View all machine columns and their descriptions by type:

- Machine
- Machine details
- Applications
- Hosting
- Connection
- Registration
- Session Details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Session

Machine

Columns in the **Machine** category.

COLUMN	DESCRIPTION	APPLIES TO
Name	The DNS host name of the machine.	Single-session and multi-session
Machine Catalog	The name of the catalog the machine belongs to.	Single-session and multi-session
Delivery Group	The name of the delivery group the machine belongs to.	Single-session and multi-session
User Display Name	The full names of the users associated with the machine (usually in the form `Firstname Lastname`). Associated users are the current users for shared machines and the assigned users for dedicated machines.	Single-session and multi-session
User	The user names of the users associated with the machine (in the form “domain\user”). Associated users are the current users for shared machines and the assigned users for dedicated machines.	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
User Principal Name	The User Principal Names of the users associated with the machine (in the form “user@domain”). Associated users are the current users for shared machines and the assigned users for dedicated machines.	Single-session and multi-session
Desktop Display Name	The published name of the machine originally used to launch the session. It’s the name displayed on the Citrix Workspace™ app or StoreFront. **Note:** To change a desktop’s display, you need the **Perform Machine Update** permission because changing the display name involves updating the machine property.	Single-session only
Desktop Conditions	The list of outstanding desktop conditions for the machine. Possible values: Unknown, CPU, ICALatency, and UPMLogonTime.	Single-session and multi-session
Allocation Type	The allocation type of the machine:	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
	Permanent, when allocated to a user permanently. **Random**, when allocated randomly.	
Maintenance Mode	Indicates whether the machine is in maintenance mode.	Single-session and multi-session
Windows Connection Setting	Logon mode reported by Windows.	Multi-session only
	Possible values: LogonEnabled, Draining, DrainingUntilRestart, and LogonDisabled.	
Is Assigned	Indicates whether a dedicated desktop has been assigned to a user or a client (name/address). Users can be assigned explicitly or by assigning-on-first-use-of-the-machine.	Single-session and multi-session
Is Physical	Indicates whether the machine is physical or not. `True` indicates that the machine is physical, meaning it isn't power-managed by DaaS. `False` indicates otherwise.	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
Provisioning Type	How the machine was provisioned. Possible values: • Manual: Not provisioned using PVS or MCS. • PVS: Provisioned using PVS (physical, blade, and virtual machines) • MCS: Provisioned using MCS (VMs only)	Single-session and multi-session
Scheduled Restart	The state of any scheduled reboot operation for the machine. Possible values: • None: No reboot is scheduled. • Pending: Awaiting reboot but is available for use. • Draining: Awaiting reboot and is	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
	unavailable for new sessions. Reconnections to existing connections are still allowed, however. • In Progress: Actively undergoing a scheduled reboot. • Natural: Natural reboot in progress. The machine is awaiting a restart.	
Zone	The name of the zone where the machine is located.	Single-session and multi-session
State	The overall state of the desktop associated with the machine, derived from various specific states such as session state, registration state, and power state.	Single-session and multi-session
	Possible states: Off, Unregistered, Available, Disconnected,	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
	InUse, and Preparing.	
Tags	The list of tags associated with the machine.	Single-session and multi-session
VDA Upgrade	The machine state for VDA package upgrade actions.	Single-session and multi-session
	Possible values: Scheduled, Not configured, Available, Up to date, Unknown.	
VDA Upgrade Status	The status for VDA upgrade actions. Possible values: Scheduled, Awaiting upgrade, In progress, Canceled, Upgrade failed, Successful, Validation failed, Unknown	Single-session and multi-session
Suspend Capable	Indicates whether the machine supports power actions (Suspend and Resume).	Single-session and multi-session
Load Evaluator Index	The current load index. The overall effective load index (percentage) for the machine. For more	Multi-session only

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
	information, see CTX202150.	
Load Index	The current load index. For more information, see Learn more.	Multi-session only
Drain State	Indicates whether the machine is draining and will shut down after all sessions on the machine end. True appears only for power-managed, multi-session machines.	Multi-session only
	Note: The machine doesn't shut down if it's in maintenance mode. It shuts down only after it's off maintenance mode.	
Cloud Connector	The name of the Cloud Connector that the machine is proxied through.	Single-session and multi-session

Machine details

Columns in the **Machine details** category.

COLUMN	DESCRIPTION	APPLIES TO
Agent Version	The version of the Citrix Virtual Delivery Agent (VDA) installed on the machine.	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
IP Address	The IP address of the machine.	Single-session and multi-session
Is Assigned	Indicates whether a dedicated desktop has been assigned to a user or a client (name/address). Users can be assigned explicitly or by assigning-on-first-use-of-the-machine.	Single-session and multi-session
OS Type	The type of the operating system running on the machine.	Single-session only

Applications

Columns in the **Applications** category.

COLUMN	DESCRIPTION	APPLIES TO
Application in Use	The list of applications in use on the machine (displayed as browser names).	Single-session and multi-session
Published Applications	The list of applications published by the machine (displayed as browser names).	Single-session and multi-session

Connections

Columns in the **Connections** category.

COLUMN	DESCRIPTION	APPLIES TO
Client (IP)	The IP address of the client connected to the machine.	Single-session only
Client	The host name of the client connected to the machine.	Single-session only

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
Plug-In Version	The version of the Citrix Workspace app on the connected client.	Single-session only
Connected Through	The host name of the incoming connection, typically a gateway, router, or client.	Single-session only
Connected Through (IP)	The IP address of the incoming connection, typically a gateway, router, or client.	Single-session only
Connection Type	The protocol used for the session. Possible values: HDX, RDP, and Console. Note: The field is left blank for console sessions on XenDesktop® 5 VDAs.	Single-session only
Last Connection Time (UTC)	The time of the last detected connection attempt that either failed or succeeded.	Single-session and multi-session
Last Connection User	The SAM name (in the form “DOMAIN\user”) of the user that last attempted a connection with the machine. If the SAM name is not available, the SID is used.	Single-session and multi-session
Secure ICA® Active	Indicates whether SecureICA is active on the current session. Always null for multi-session machines.	Single-session and multi-session

Hosting

Columns in the **Hosting** category.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
VM	The friendly name of a hosted machine running the session, as used by its hypervisor. It doesn't necessarily match either the DNS or AD name of the machine.	Single-session and multi-session
Hosting Server Name	The DNS name of the hypervisor that is hosting the machine if managed.	Single-session and multi-session
Connection	The name of the host connection assigned to the machine hosting the session.	Single-session and multi-session
Pending Update	Indicates whether the VM image for a hosted machine is out of date and due to be updated to a new image at the machine's next reboot.	Single-session and multi-session
User Change Persistence	How user changes are handled, indicating whether the changes are persistent: • OnLocal: Persistent. User changes are saved locally.	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
	• Discard: Non-persistent. User changes are discarded.	
Pending Power Action	Indicates whether there are any pending power actions for the machine.	Single-session and multi-session
Power State	The power state of the machine. Possible values: Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.	Single-session and multi-session
Will Shut Down After Use	Applicable only to power-managed, single-session machines. Indicates whether the machine is tainted and will shut down after all sessions end. **Note:** The machine won't shut down if it's in maintenance mode. It will shut down only after it is taken out of maintenance mode.	Single-session only

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Registration

Columns in the **Registration** category.

COLUMN	DESCRIPTION	APPLIES TO
Last Registration Failure	The reason for the last deregistration of the machine with the broker. Possible values are: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart,	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
	DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError, and BrokerRegistrationLimitReached.	
Last Registration Failure Time (UTC)	The time of the last deregistration of the machine.	Single-session and multi-session
Registration State	The registration state of the machine. Possible values: Unregistered, Initializing, Registered, and AgentError.	Single-session and multi-session
Fault State	The summary state of any current fault state of the machine. Possible values: • None: No fault. The machine is healthy. • FailedToStart: The last power-on operation for	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
	the machine failed. • StuckOnBoot: The machine failed to start after being powered on. • Unregistered. The machine failed to register within the expected period or its registration has been rejected. • MaxCapacity. The machine is reporting itself at maximum capacity.	

Session details

Columns in the **Session details** category.

COLUMN	DESCRIPTION	APPLIES TO
Launched Over	The host name of the StoreFront server used to launch the current brokered session. Always null for multi-session machines.	Single-session and multi-session
Launched Over (IP)	The IP address of the StoreFront server used to launch the current brokered	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION	APPLIES TO
	session. Always null for multi-session machines.	
Session Change Time (UTC)	The time of the last state change of the current session.	Single-session only
SmartAccess Filters	Smart Access tags for the current session. Always null for multi-session machines.	Single-session and multi-session

Session

Columns in the **Session** category.

COLUMN	DESCRIPTION	APPLIES TO
Session State	The state of the current session. Possible values: Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession, and Unknown.	Single-session only
Current User	The name of the current session’s user (in the form “DOMAIN\user”).	Single-session only
Start Time (UTC)	The start time of the current session.	Single-session only
Session Count	The number of sessions on the machine.	Multi-session only

Session actions and columns

This article lists session actions, session columns, and their descriptions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Actions

View the actions you can perform on sessions and their descriptions. Some actions support the **Select all** operation, allowing you to apply the action to all sessions across all pages.

ACTION	DESCRIPTION	APPLIES TO SESSIONS ON
Log off	Log a user off a session.	Single-session OS machines or multi-session OS machines
Send Message	Send a message to the user of a session.	Single-session OS machines or multi-session OS machines
View machines	View the hosting machine for a session.	Single-session OS machines or multi-session OS machines
Disconnect	Disconnect a session. If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the DaaS.	Single-session OS machines or multi-session OS machines
Shut Down Machine	Shut down the machine associated with a session.	Single-session OS machines
Restart Machine	Restart the machine associated with a session.	Single-session OS machines

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION	APPLIES TO SESSIONS ON
View in Monitor	Open the detailed view of a machine in Monitor. This action is available only to roles with the **Director > Manage > View Activity Manager page** or the **Director > Manage > View User Details page** permission.	Single-session and multi-session OS machines

Columns

View session columns and their descriptions.

COLUMN	DESCRIPTION
Current user	The name of the user; the User Principal Name (UPN) of the user.
Name	The DNS host name of the machine hosting the session.
Delivery Group	The name of the delivery group containing the session’s hosting machine.
Machine Catalog	The name of the machine catalog containing the session’s hosting machine.
Agent Version	The version of the Citrix Virtual Delivery Agent (VDA)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION
	installed on the machine hosting the session.
Application in Use	The list of applications in use in the session, identified by their administrative names.
Autonomously Brokered	Whether this is an HDX™ session established by a direct connection without being brokered.
Brokering Time (UTC)	The time at which the session was brokered.
Brokering User Name	The name of the brokering user.
Client (IP)	The IP address of the client connected to the session.
Client	The host name of the client connected to the session.
Plug-In Version	The version of Citrix Workspace™ app running on the client connected to the session.
Connected Through	The host name of the incoming connections, typically a gateway, router, or client.
Connected Through (IP)	The IP address of the incoming connection, typically a gateway, router, or client.
Allocation Type	Whether the session is shared or dedicated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION
Hidden	Whether the session is hidden from the user and not to be reconnected to.
VM	The friendly name of the VM hosting the session, as used by its hypervisor. It doesn't necessarily match either the DNS or AD name of the machine.
Hosting Server Name	The DNS name of the hypervisor that is hosting the session's hosting machine.
Connection	The name of the host connection assigned to the machine hosting the session.
Pending Update	Whether the VM image for a hosted machine is out of date and due to be updated to a new image at the machine's next reboot.
Maintenance Mode	Whether the machine hosting the session is in maintenance mode.
IP Address	The IP address of the machine hosting the session.
Is Physical	Whether the machine hosting the session is physical or not. `True` indicates that the machine is physical, meaning it isn't power-managed by DaaS. `False` indicates otherwise.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION
Launched Over	The host name of the StoreFront™ server used to launch the session. Blank if the session was launched via Workspace.
Launched Over (IP)	The IP address of the StoreFront server used to launch the session. Blank if the session was launched via Workspace.
OS Type	The identification string of the operating system hosting the session.
User Change Persistence	How user changes are handled, indicating whether the changes are persistent: • OnLocal: Persistent. User changes are saved locally. • Discard: Non-persistent. User changes are discarded.
Connection Type	The protocol used for the session, such as HDX, RDP, or Console. **Note:** The field is blank for console sessions on XenDesktop® 5 VDAs.
Provisioning Type	How the machine hosting the session was provisioned:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION
	• Manual: Not provisioned using PVS or MCS. • PVS: Provisioned by PVS (Physical, blade, and virtual machines). • MCS: Provisioned by MCS (VMs only).
Secure ICA® Active	Whether SecureICA is active on the session.
Session State	The state of the session. Possible values: Connected, Active, or Disconnected. Other states might occur for sessions on machines with functional levels earlier than L7, such as PreparingSession, Reconnecting, NonBrokeredSession, Other, and Unknown.
Session Change Time	The time of the most recent state change for the session.
Application State	The state of applications in the session. Possible values: PreLogon, PreLaunched, Active, Desktop, Lingering, and NoApps.
Session Support	Whether the machine hosting the session supports multiple or single sessions.
Zone	Name of the zone where the machine hosting the session is located.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION
SmartAccess Filters	Smart Access tags for the session.
Start Time (UTC)	When the session was started.
State	The summary state of the machine. Possible values: Unregistered, Disconnected, or InUse.
Time in State (UTC)	How long the session has been in its current state.
Delivery Controller™	The DNS host name of the controller that the session's hosting machine is registered with.
User Display Name	The full name of the user.
Desktop Display Name	The published name of the machine originally used to launch the session. It's the name displayed on the Citrix Workspace app or StoreFront. For application sessions, it's the name of the first application launched into the session even if that application has since ended. The name keeps unchanged even if the resource is later renamed or removed.

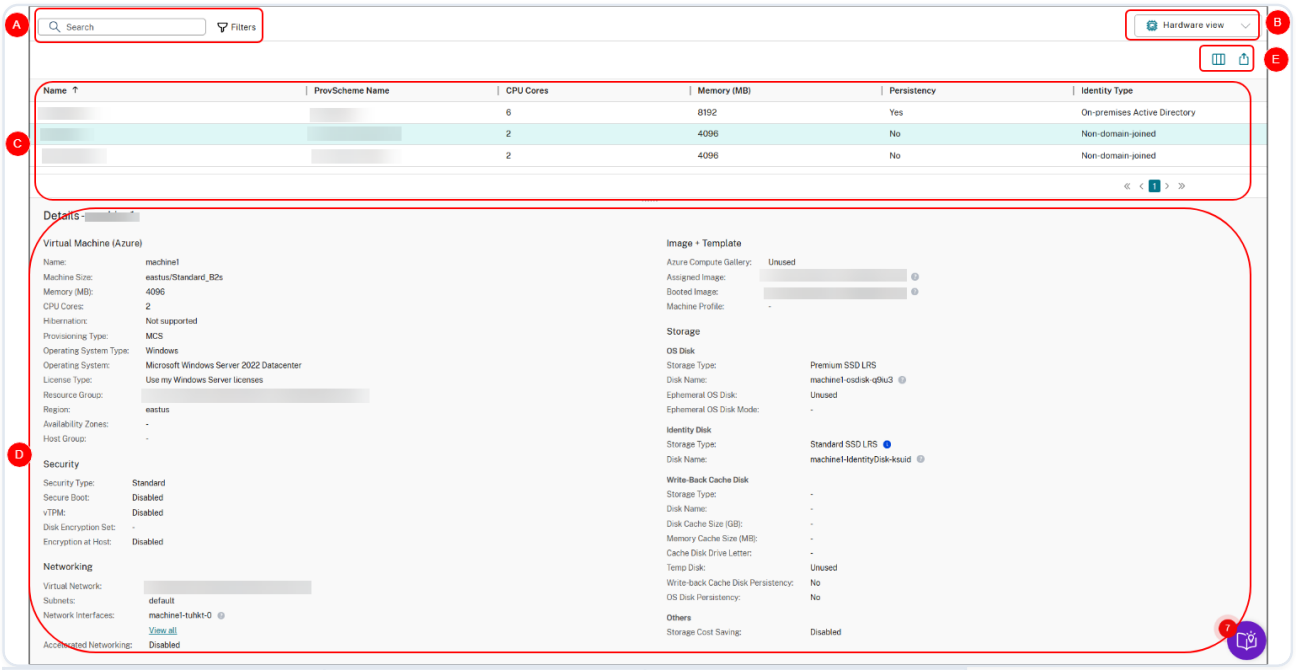
Monitor MCS-provisioned machines in Search > Hardware view

This article guides you through how to view MCS-provisioned machines and their properties using the **Hardware view** within the **Search** node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Learn about the hardware view

The hardware view within the **Search** node displays your MCS-provisioned machines and their critical properties, including machine security settings, network details, images, and machine profile details.



CALLOUT	AREA	DESCRIPTION
A	Search bar	Provides a quick search and a filter-based search that allows you to define complex search criteria. For more information, see Search for machines. **Tip:** Use filters to quickly narrow down machines by specific properties. For example, combine **Pending Image Update = Yes** and **Identity Type = ActiveDirectory** to view all Active

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CALLOUT	AREA	DESCRIPTION
		Directory machines that are pending image updates.
B	Switch to Default view	Switch from Hardware view to Default view.
C	Main view	Displays your MCS-provisioned machines and their critical properties. You can customize the view by selecting the **Column to display** icon. For more information about available columns, see Machine columns.
D	Details pane	Displays detailed information for the selected machine.
E	List-level actions	Displays actions that you can perform on the entire displayed list: • **Export** icon: Export the list of machines displayed in the main view to a CSV file. • **Column to display** icon: Customize the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CALLOUT	AREA	DESCRIPTION
		main view for the list.

Reference: Machine columns

This table lists all columns in Hardware view and their descriptions.

COLUMN	DESCRIPTION
Name	The DNS host name of the machine.
Provisioning Scheme Name	The name of the provisioning scheme used to provision the machine.
CPU Cores	The number of CPU cores allocated to the machine.
Memory (MB)	The amount of memory (in MB) allocated to the machine.
Persistency	Indicates whether the machine's disk and data persist across restarts.
Identity Type	The identity type of the machine.
Pending Image Update	Indicates whether the VM image for the machine is outdated and due to be updated to a new image at the machine's next reboot.
Last Boot Time (UTC)	The date and time (in UTC) when the machine was last started.
Use WBC	Indicates whether the machine is configured with WBC (aka MCSIO).
WBC Disk Size (GB)	The MCSIO disk-cache size of the machine.
WBC Memory Size (MB)	The MCSIO memory-cache size of the machine.
Identity Provider	The identity provider of the machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION
Activation Type	Valid only for Windows VDAs. The Windows license activation type of the machine. Values include: Unsupported VDA, Key Management Service, Multiple Activation Key, and Not valid.

Multi-site management and user resource aggregation

As an administrator with full access to multiple sites, you can designate one site as the primary and link other sites to it for centralized management. This feature helps improve operational efficiency across various aspects:

- **Efficient site management**. Administrators can manage multiple sites from a single interface, switching between them using the drop-down menu in the upper-right corner.
- **Seamless navigation**. Administrators can seamlessly switch between Studio and Monitor without needing to reselect the site. When a site is selected in Studio, it's automatically selected in Monitor, streamlining your workflow.
- **Simplified help desk operations**. Administrators can view information for all sites in one Monitor console.
- **Aggregated end-user resources**. End users can sign in to a single store (*for example*, primarysite.cloud.com) to access their apps and desktops from any linked site.

This article helps you understand, configure, and use centralized site management. It guides you through the following topics:

- Overview
- Best practices for multi-site management
- Full access administrators: Set up centralized site management
- Administrators: Manage sites from a single interface
- Typical use cases

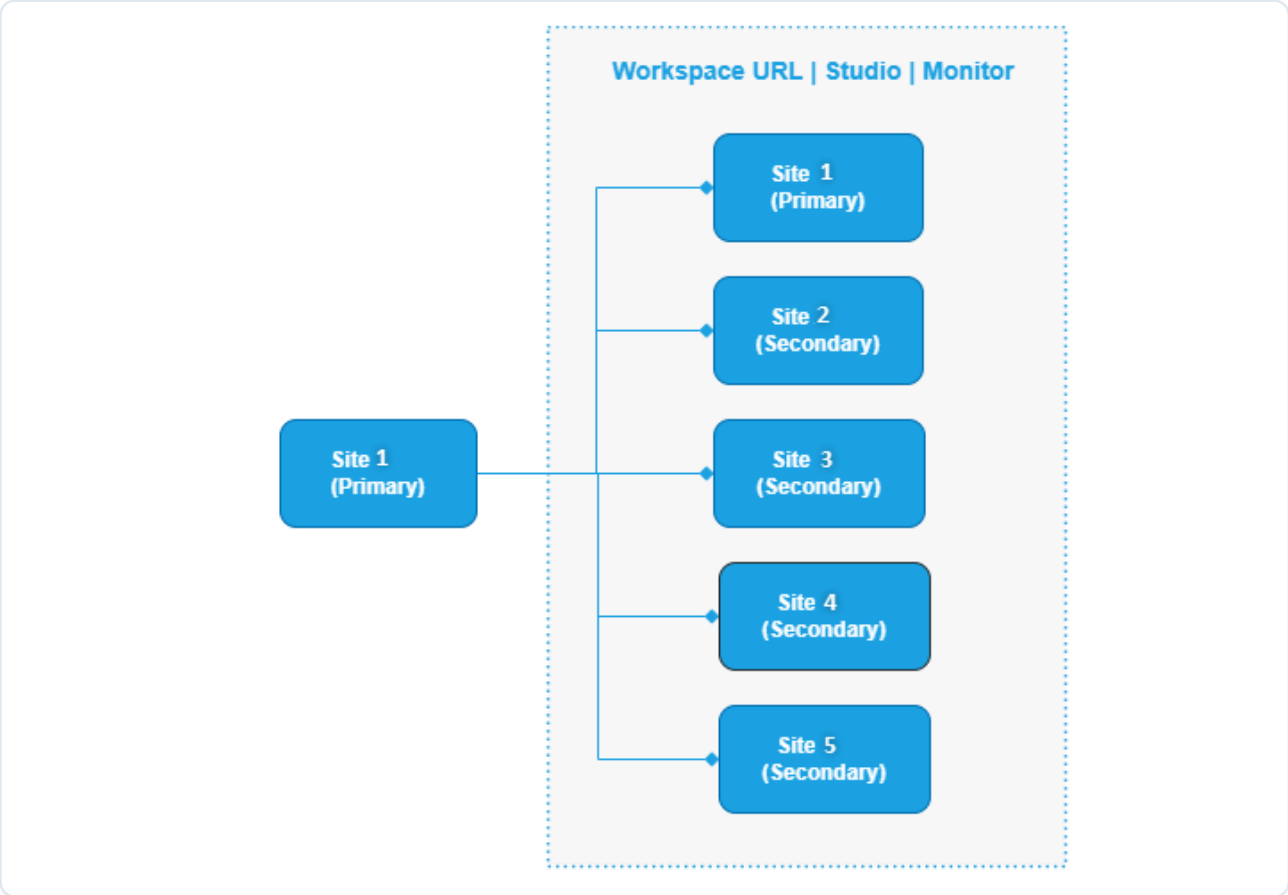
NOTE:

Centralized site management is currently not supported for Citrix Service Providers (CSPs) and their tenants.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overview

The following diagram illustrates the hierarchical primary-secondary architecture in centralized site management.



Primary and secondary sites definitions:

- **Primary** (also known as **hub**). The central site used to manage all linked sites.
- **Secondary** (also known as **spoke**). A site added to the primary site for centralized management.

Administrator roles and permissions

Access to the multi-site management feature varies based on the administrator role:

- Only administrators with **full access** can set up multi-site management and end-user resource aggregation.
    - For sites to be managed as secondary sites, the current administrator must have full access to those sites.
- After setup:
    - In the **Studio** console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - If you're a primary site administrator (either custom or full access administrator), you can view the secondary sites in the site drop-down list at the top right corner of the Studio console after accessing the primary site. The list includes secondary sites where you're an administrator with **DaaS console access**.

  - In the **Monitor** console

    - Multi-site management is available only to administrators with the **Help Desk Administrator** or the **Full Monitor Administrator** role.

Limitations

- **Limit to four secondary sites.** For optimal performance in aggregating end-user resources through a single store URL, we recommend adding no more than four secondary sites. For example, exceeding this limit might lead to slow sign-ins in Monitor.
- **Microsoft Entra ID (Azure AD) administrator groups.** For Microsoft Entra ID administrator groups to work properly with multi-site management, allow Entra ID group members to switch between Citrix Cloud accounts. To do so, link the accounts that you want administrators to switch between. For more information about Microsoft Entra ID (Azure AD) administrator groups, see Manage administrator groups.

NOTE:

- After linking the accounts using the script-based approach, the **Add DaaS Sites** page defaults to the **Add DaaS sites and aggregate end-user resources through a single store URL** option. Do not switch to the **Add DaaS sites only** option. Doing that will unlink the accounts, reverting the account link that was created using the script. As a result, the multi-site management will not work as expected.
- Multi-site management requires that the Entra ID administrator group has full access.

Best practices for multi-site management

To ensure a consistent multi-site management experience, we strongly recommend setting up the feature as follows:

1. Define the account structure.

   a. Identify a primary cloud account (hub).

   b. Identify secondary cloud accounts (spokes) to link.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. (Needed only for Microsoft Entra ID administrator groups) Link the primary and secondary accounts.

   For more information, see Linking the accounts using the script-based approach.

3. Set up multi-site management.

   Required access: Administrator with **full access** to the primary and secondary sites.

   a. Sign in to **Citrix Cloud** and select the *primary account* from the account list.
   b. In the DaaS management console (Studio), go to **Settings > Site settings** and click **Add** in the **Centralize site management** tile.
   c. Select the secondary sites. For more information, see Set up centralized site management.

   After the configuration is complete, a site drop-down list appears in the upper-right corner of the Studio and Monitor consoles.

4. Manage a secondary site.

   Required access: Administrator with full or custom access to the primary and secondary sites.

   a. Sign in to **Citrix Cloud** and select the *primary account* from the account list.
   b. Access a secondary site using the site drop-down list.
   c. Manage this site using the left navigation menu.

Full access administrators: Set up centralized site management

As an administrator with **full access** to multiple sites, you can set up centralized site management for those sites.

Preparation

Before you begin, you need to:

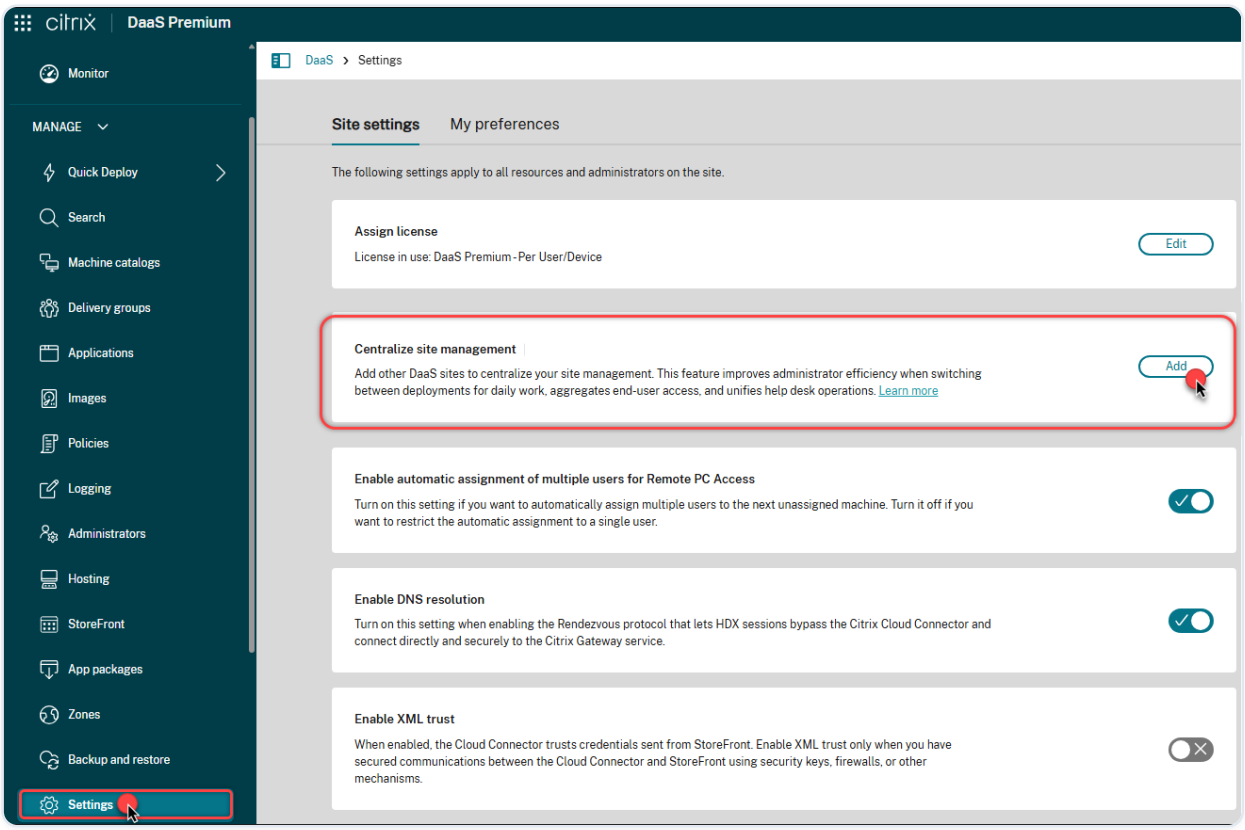
- **Designate a primary cloud account**. Determine a cloud account (also called *site*) where you centrally manage sites in your organization.
- **Ensure you have full access**. Ensure that you have full access to all sites you want to link for centralized management. For more information, see Add an administrator.

Set up centralized site management

To set up centralized site management, follow these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Sign in to **Citrix Cloud™**, and then select the cloud account that you want to designate as the *primary* site.
2. Access **DaaS** to open Studio.
3. In the left pane, select **Settings**.
4. On the **Site settings** tab, click **Add** in the **Centralize site management** tile.



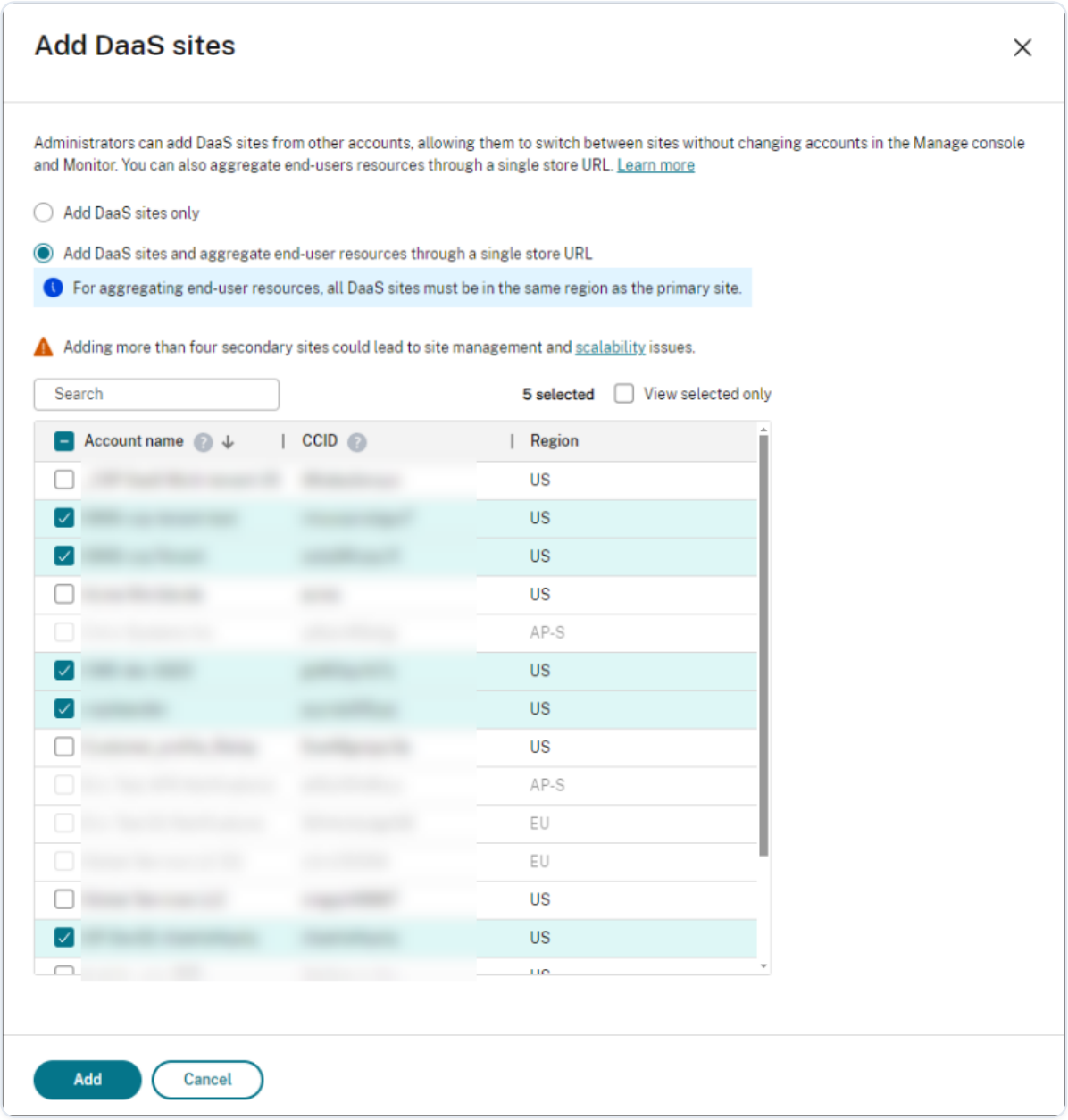
5. On the **Acknowledge** page that appears, select the confirmation checkbox and click **Confirm** to confirm configuring this site as the primary.
6. On the **Add DaaS sites** page that appears, complete the following settings:

   a. Select how you want to apply the centralized management:

      - **Add DaaS sites only**. Apply centralized management only to the Studio and Monitor consoles.
      - **Add DaaS sites and aggregate end-user resources through a single store URL**. Apply centralized management to both the Studio and Monitor consoles and the store URL.

   b. Select the cloud accounts that you want to add as secondary sites. Only cloud accounts to which you have **full access** appear.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

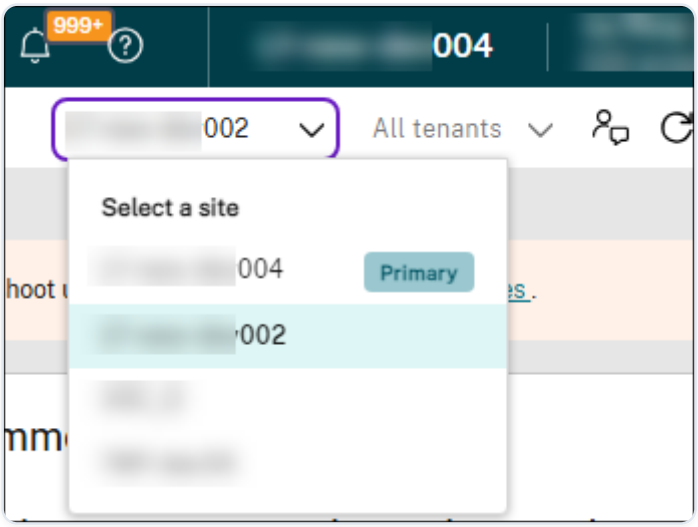
If you chose **Add DaaS sites and aggregate end-user resources through a single store URL** in the previous step:

- For optimal performance in aggregating end-user resources, we recommend adding no more than four secondary sites.
- Only those sites located in the same region as the primary site are available for selection as secondary sites.

c. Click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Refresh your browser. The site selection box appears at the top right corner of the console, where this site and its secondary sites appear.



NOTE

- After setup, multi-site management is available to administrators of the designated primary site, enabling them to manage secondary sites from a single Studio UI without switching accounts. For more information, see manage multiple sites from a single Studio UI.
- You can also enable multi-site management for other sites in the aggregation, designating that site as a primary site.
- Centralized site management isn't supported for CSPs and their tenants, even though the **Add** or **Manage** button on the **MANAGE > Settings > Centralize site management** tile is enabled.

Add or remove a secondary site

As an administrator with **full access** to the primary site, you can add or remove a secondary site from the centralized site management. Detailed steps are as follows:

1. Sign in to Citrix Cloud and select the account name of the *primary site*.
2. Access **DaaS** to open Studio.
3. In the left pane, select **Settings**.
4. In the **Centralize site management** tile, click **Manage**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. On the **Manage DaaS sites** page that appears, clear the checkbox next to the account you want to detach from the primary site or select the one you want to add to the primary site.
6. Click **Save**.

NOTE:

When you switch to a *secondary* site through the *primary* site, the **Manage** button on the **MANAGE > Settings > Centralize site management** tile is disabled.

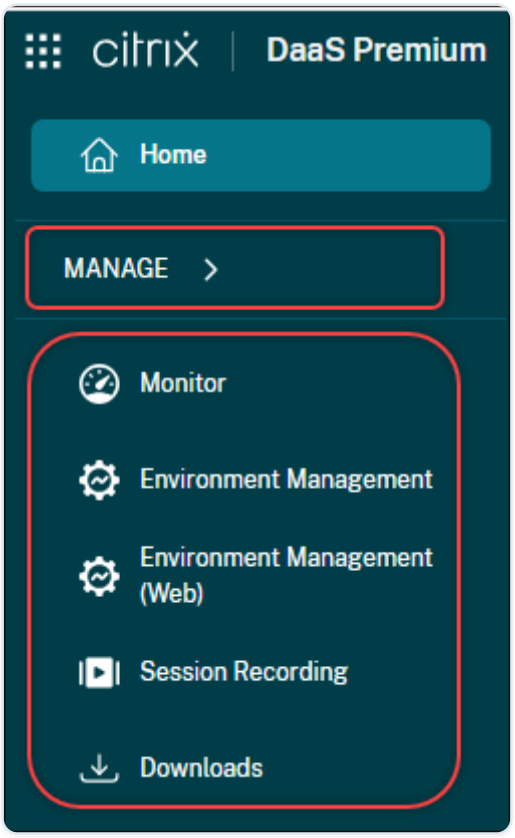
Administrators: Manage sites from a single interface

After setup, as an administrator (either custom or full access) of multiple sites, you can manage them from *one* Studio UI, eliminating the need to change accounts.

Considerations when switching between sites

- Each site's configuration is managed separately. Settings from one site don't merge with another in the **Manage** menu.
- When you are on a *secondary* site from the *primary* site:
  - Your access to menu items in the **MANAGE** menu depends on your permissions for the *secondary* site.
  - Your access to menu items *other than* **MANAGE** in the left pane depends on your permissions for the *primary* site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Manage sites

To manage sites from a single interface, follow these steps:

1. Sign in to Citrix Cloud and select the account name of the *primary* site.
2. Access **DaaS** to open Studio.
3. Select a site as needed from the site drop-down list in the upper-right corner. The drop-down list includes the primary site and any secondary sites where you have an administrator role with **DaaS console access**.
4. From the left pane, select a node under **Manage** and start your management. *For example*, select **Machine Catalogs** to start creating or managing catalogs for the selected site.

Administrators: Monitor sites from a single interface

After setup, as a Help Desk Administrator or Full Monitor Administrator of multiple sites, you can monitor them from *one* Monitor UI, eliminating the need to change accounts.

Typical use cases

Centralized site management helps organizations simplify administration and user access across multiple Citrix DaaS™ sites. This section outlines common use cases.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Efficient site administration

Multi-site management simplifies administration. For example, an organization with three DaaS sites can manage them centrally:

- Site A: Development
- Site B: User Acceptance Testing
- Site C: Production

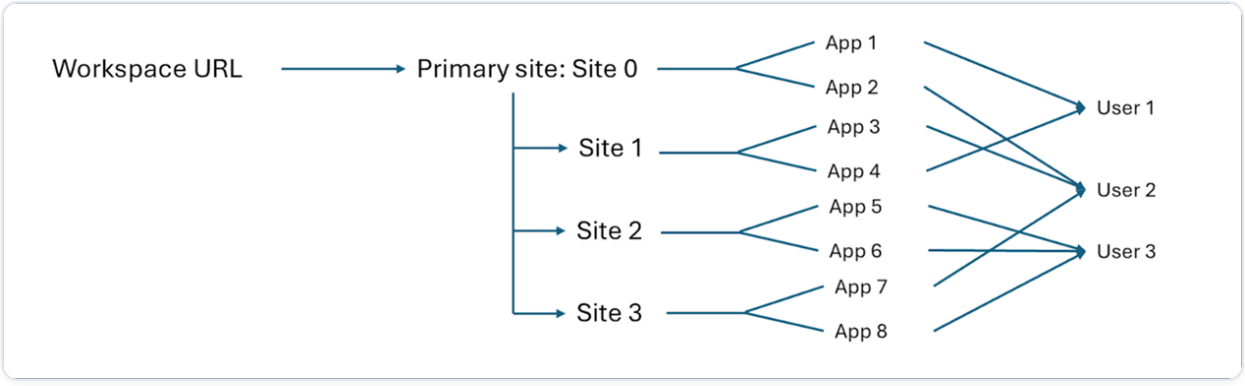
Mergers and acquisitions

Acquiring a new company often results in a complex domain structure, such as multiple FQDN domains from different forests with the same name in a domain trust. A single site might cause resource enumeration or access issues. Multi-site management enables organizations to maintain separate deployments while managing them from a single interface.

End-User resource aggregation

With end-user resource aggregation enabled, users can access apps and desktops from multiple sites through the primary site's store URL. For example:

- Without aggregation: User 2 must use separate URLs for each site:
  - Site 0 store URL to access App 2
  - Site 1 store URL to access App 3
  - Site 3 store URL to access App 7
- With aggregation: User 2 accesses all apps through the primary site’s store URL.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage personal preferences in Studio

Use the **My preferences** tab under the **Settings** node to manage your personal view and interaction preferences in Studio. These settings apply only to your account and do not affect other administrators. Available options include:

- **Date and time**: Set your default time zone, date format, and time format. These settings are used throughout Studio for time-related displays, such as scheduled restarts and autoscaling.
- **Folder view**: Choose whether to show or hide the folder view in the **Machine Catalogs**, **Delivery Groups**, and **Applications** nodes.
- **Tab order in Search**: Customize the tab order within the **Search** node.

To set your preferred view in Studio, follow these steps:

1. In Studio, go to **Settings > My preferences**.
2. Click **Edit**.
3. In the **Date and time** tile, configure the following format settings:
    - **Date format**: Select how to display the date (for example, yyyy/MM/dd). To use the date format associated with the language you chose for Studio, select **Match console language**.
    - **Time format:** Select a 12-hour format (09:00 PM, for example) or a 24-hour clock (21:00, for example). To use the time format associated with the language you chose for Studio, select **Match console language**.
    - **Time zone:** Select your preferred time zone. To use your computer's time zone, select **Match console language**.

    NOTE:

    - To use your computer's regional settings for date, time, or time zone, select **Match console language**.
    - Int Studio, you can hover over any displayed time to view its equivalent in your local time zone.
4. In the **Folder view** tile, select whether to show or hide the folder view in the **Machine Catalogs**, **Delivery Groups**, and **Applications** nodes.
5. In the **Tab order in Search** tile, drag and reorder the tabs within the **Search** node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Click **Apply** to save and apply the changes immediately.

Security keys

NOTE:

- You must use this feature in combination with StoreFront™ 1912 LTSR CU2 or later.
- The Secure XML feature is supported only on Citrix ADC and Citrix Gateway release 12.1 and later.

This feature lets you allow only approved StoreFront and Citrix Gateway machines to communicate with Citrix Delivery Controllers. After you enable this feature, any requests that do not contain the key are blocked. Use this feature to add an extra layer of security to protect against attacks originating from the internal network.

A general workflow to use this feature is as follows:

1. Display security key settings in Studio. (Use the Remote PowerShell SDK)
2. Configure settings for your deployment. (Use Studio or Remote PowerShell SDK).
3. Configure settings in StoreFront. (Use PowerShell).
4. Configure settings in Citrix ADC.

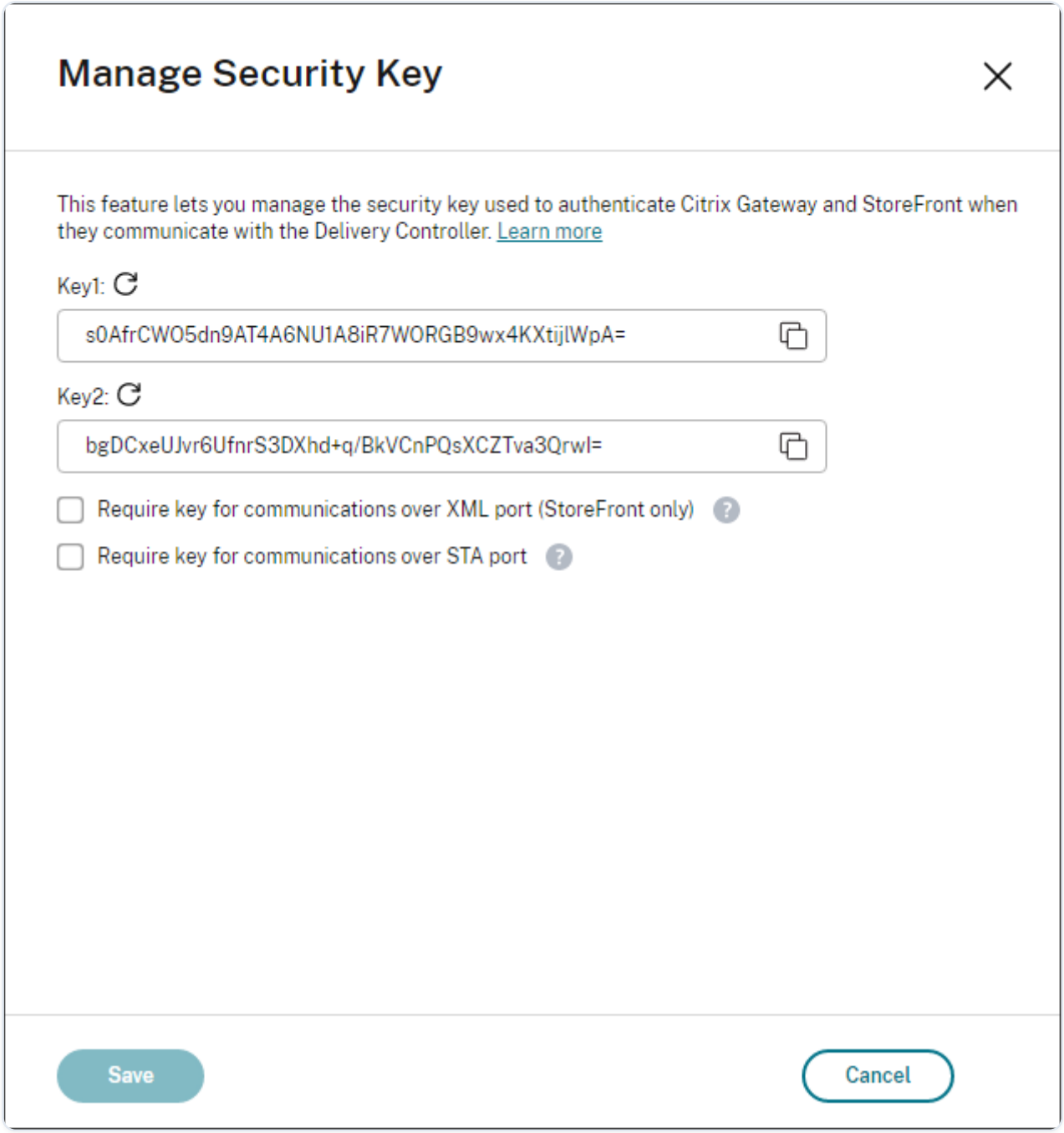
Configure settings for your deployment

You can configure settings for your deployment by using Studio or PowerShell.

Use Studio

After enabling the feature, navigate to **Settings > Site settings > Manage security key** and click **Edit**. The **Manage Security Key** blade appears. Click **Save** to apply your changes and to exit the blade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



IMPORTANT:

- There are two keys available for use. You can use the same key or different keys for communications over the XML and STA ports. We recommend that you use only one key at a time. The unused key is used only for key rotation.
- Do not click the refresh icon to update the key already in use. If you do, service interruption will occur.

Click the refresh icon to generate new keys.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Require key for communications over XML port (StoreFront only). If selected, require a key to authenticate communications over the XML port. StoreFront communicates with Citrix Cloud over this port. For information about changing the XML port, see Knowledge Center article CTX127945.

Require key for communications over STA port. If selected, require a key to authenticate communications over the STA port. Citrix Gateway and StoreFront communicate with Citrix Cloud over this port. For information about changing the STA port, see Knowledge Center article CTX101988.

After applying your changes, click **Close** to exit the **Manage Security Key** blade.

Use the Remote PowerShell SDK

The following are PowerShell steps equivalent to the operations performed in Studio.

1. Run the Remote PowerShell SDK.
2. In a command window, run the following command:
   - `Add-PSSnapIn Citrix*`
3. Run the following commands to generate a key and set up Key1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Run the following commands to generate a key and set up Key2:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Run one or both of the following commands to enable the use of a key in authenticating communications:
   - To authenticate communications over the XML port:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - To authenticate communications over the STA port:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

See the PowerShell command help for guidance and syntax.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure settings in StoreFront

After completing the settings for your deployment, you need to configure relevant settings in StoreFront by using PowerShell.

On the StoreFront server, run the following PowerShell commands:

To configure the key for communications over the XML port, use command Set-STFStoreFarm. For example:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

Enter the appropriate values for the following parameters:

- `Path to store`
- `Resource feed name`
- `secret`

To configure the key for communications over the STA port, use the `New-STFSecureTicketAuthority` and `Set-STFRoamingGateway` commands. For example:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

Enter the appropriate values for the following parameters:

- `Gateway name`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `STA URL`
- `Secret`

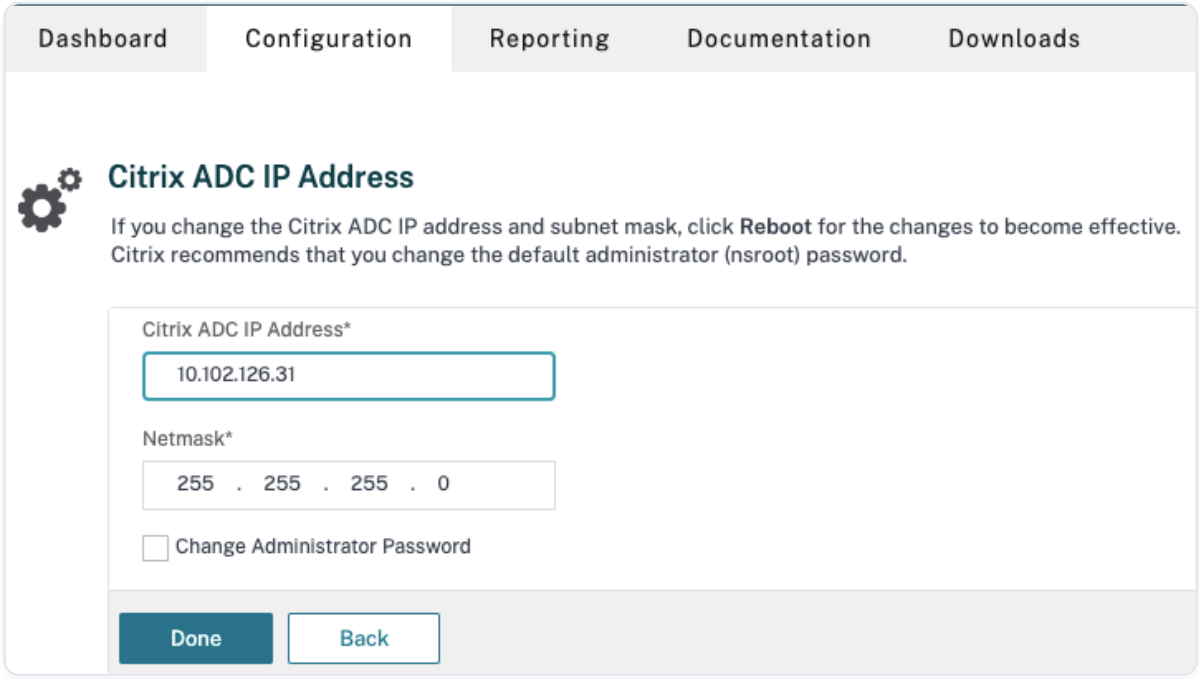
See the PowerShell command help for guidance and syntax.

Configure settings in Citrix ADC

NOTE:

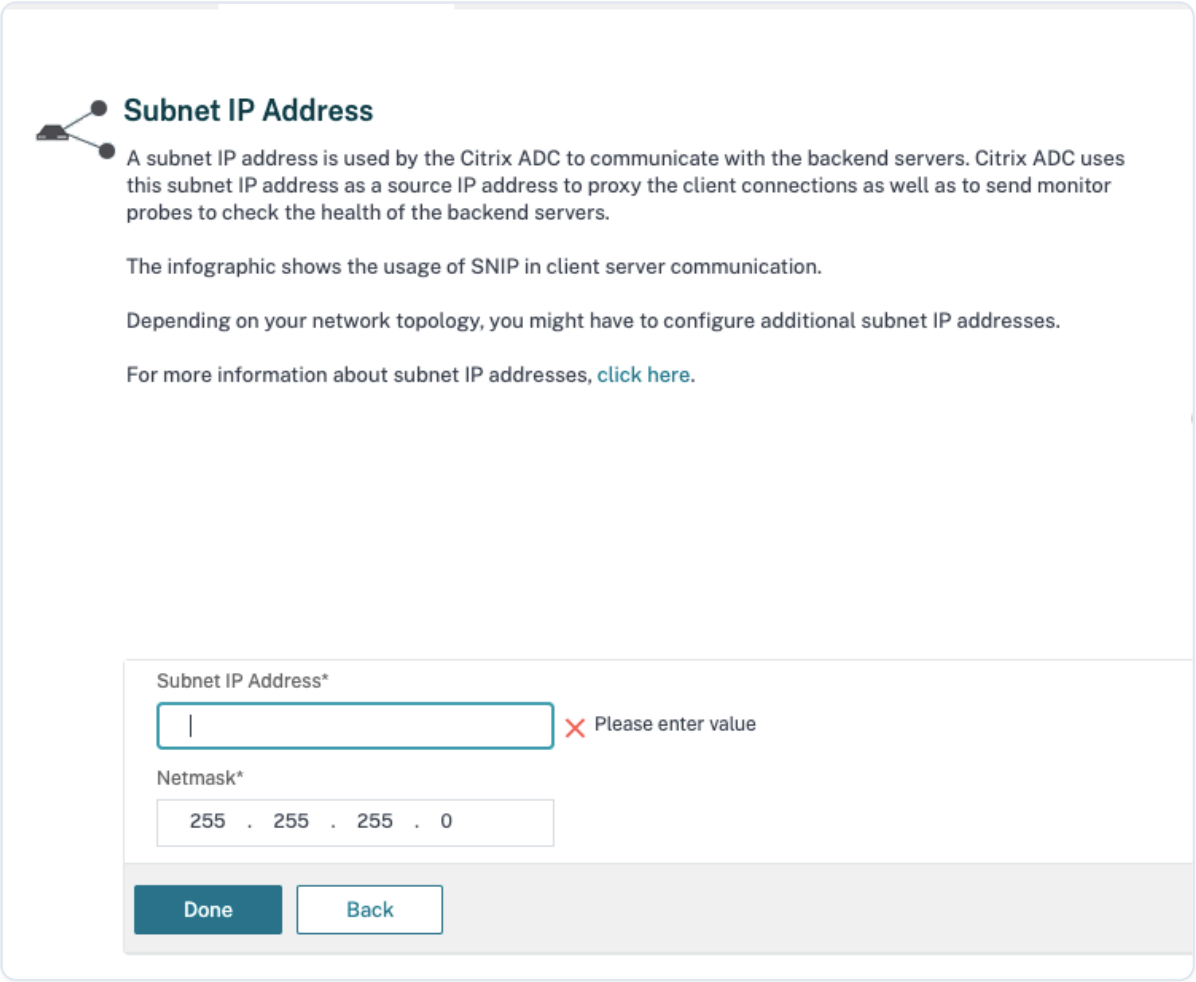
Configuring this feature in Citrix ADC is not required unless you use Citrix ADC as your gateway. If you use Citrix ADC, follow the steps below.

1. Ensure that the following prerequisite configuration is already in place:
   - The following Citrix ADC related IP addresses are configured.
     - Citrix ADC Management IP (NSIP) address for accessing the Citrix ADC console. For details, see Configuring the NSIP address.



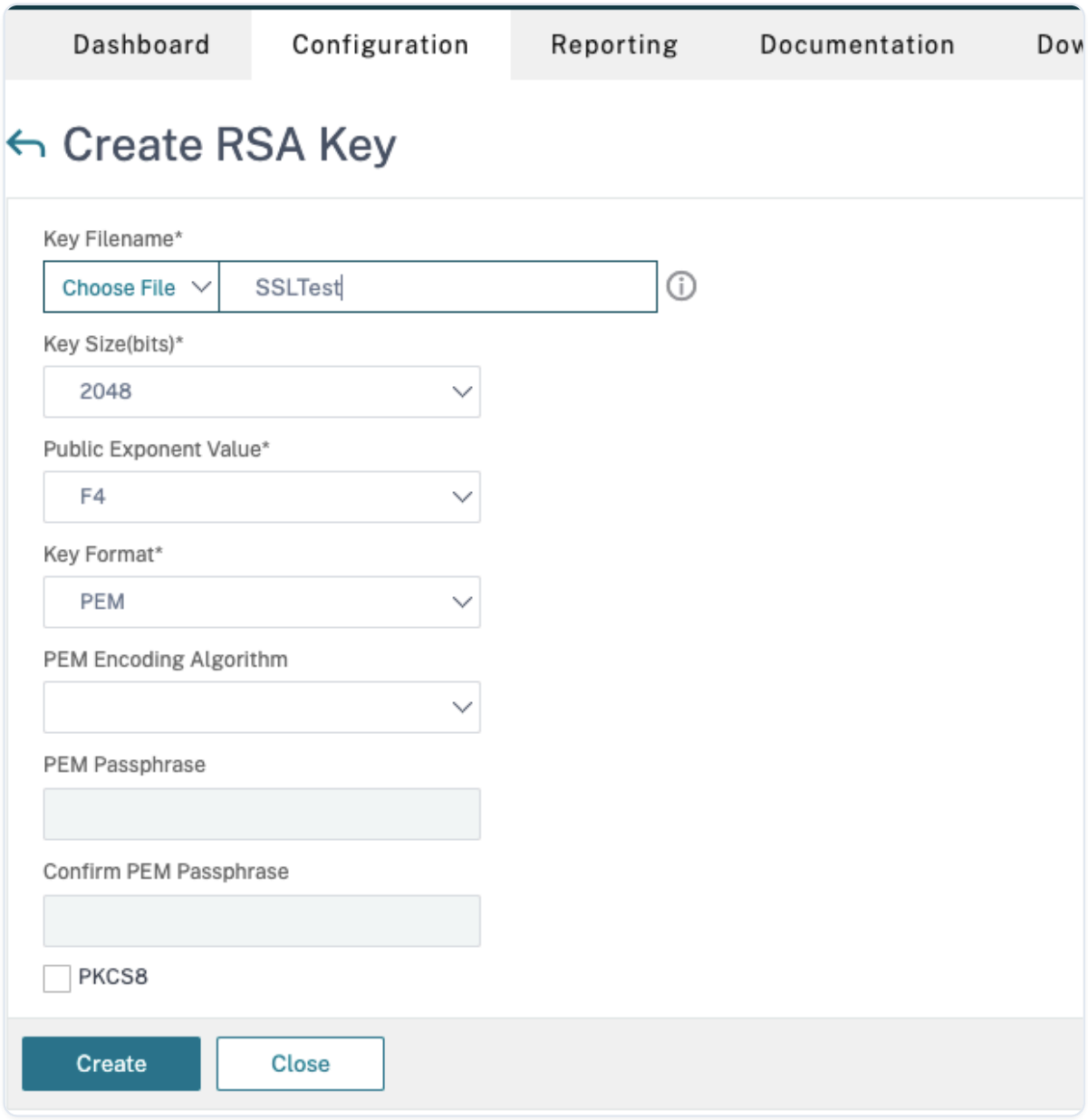
     - Subnet IP (SNIP) address for enabling communication between the Citrix ADC appliance and the back-end servers. For details, see Configuring Subnet IP Addresses.
     - Citrix Gateway virtual IP address and load balancer virtual IP address to log in to the ADC appliance for session launch. For details, see Create a virtual server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



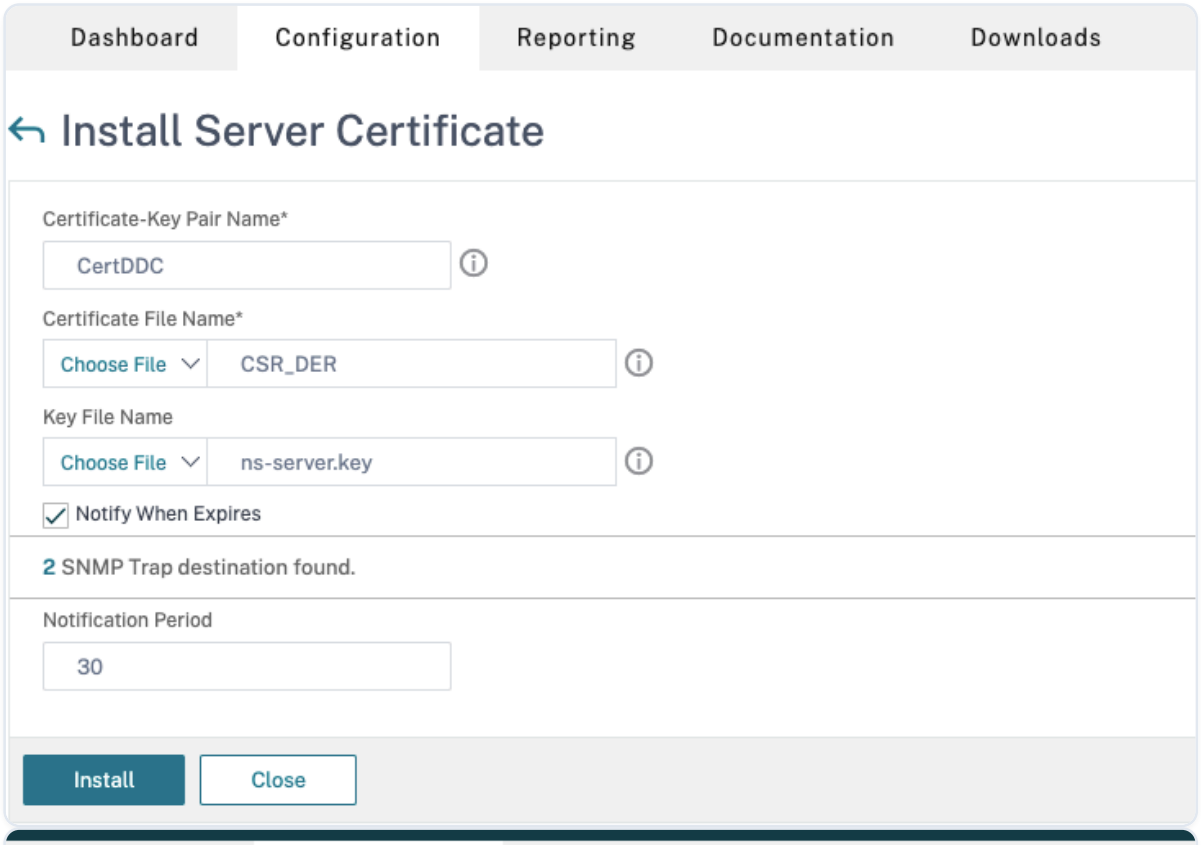
- The required modes and features in the Citrix ADC appliance are enabled.
  - To enable the modes, in the Citrix ADC GUI go to **System > Settings > Configure Mode**.
  - To enable the features, in the Citrix ADC GUI go to **System > Settings > Configure Basic Features**.
- Certificates related configurations are complete.
  - The Certificate Signing Request (CSR) is created. For details, see Create a certificate.

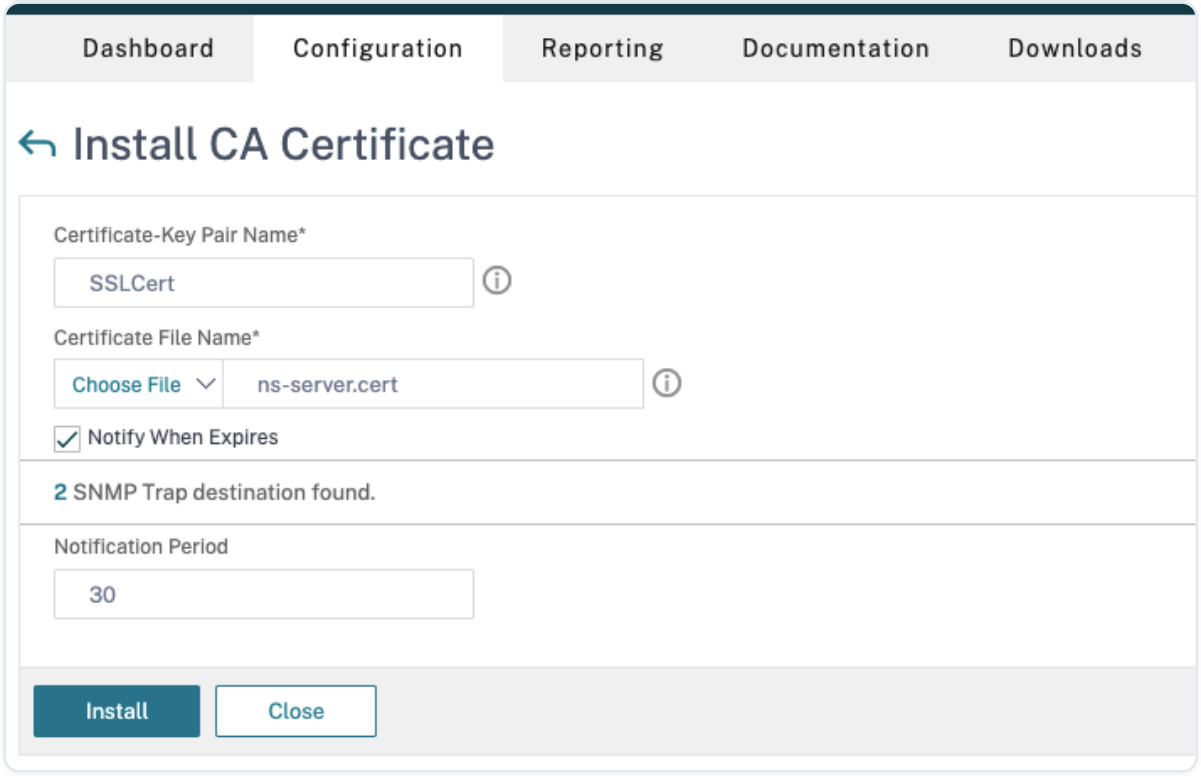
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The server and CA certificates and root certificates are installed. For details, see Install, link, and updates.

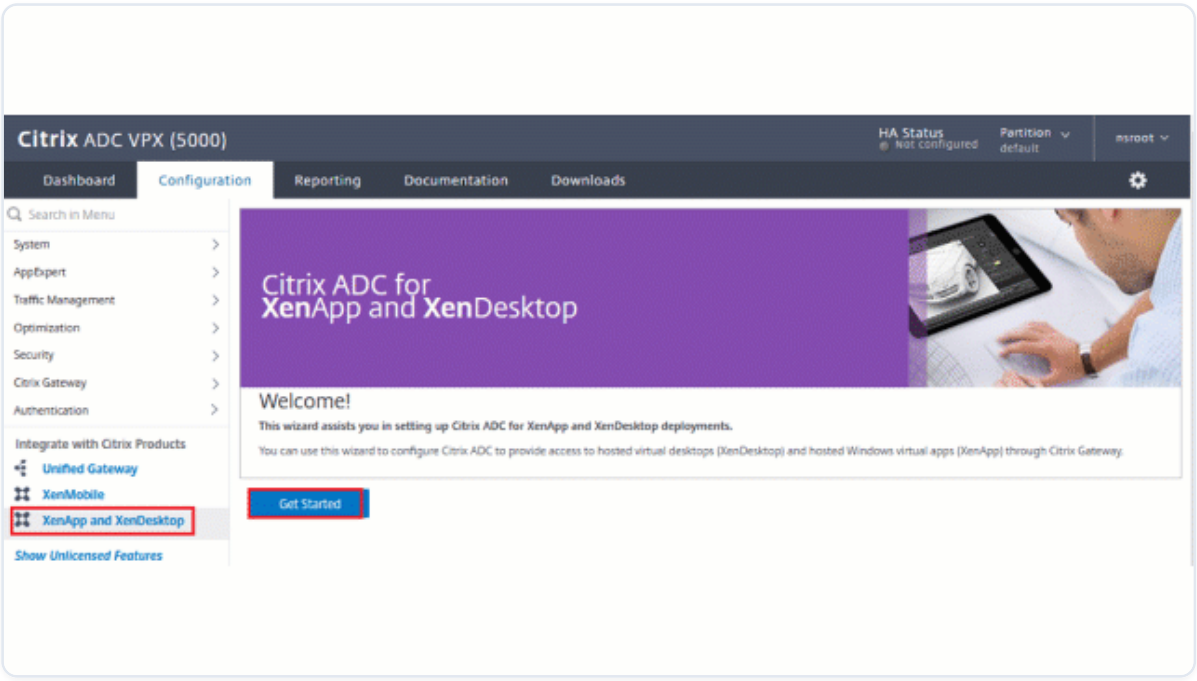
© 1997–2026 Citrix Systems, Inc. All rights reserved.





- A Citrix Gateway has been created for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Test the connectivity by clicking the **Test STA Connectivity** button to confirm that the virtual servers are online. For details, see Setting up Citrix ADC for Citrix Virtual Apps and Desktops.

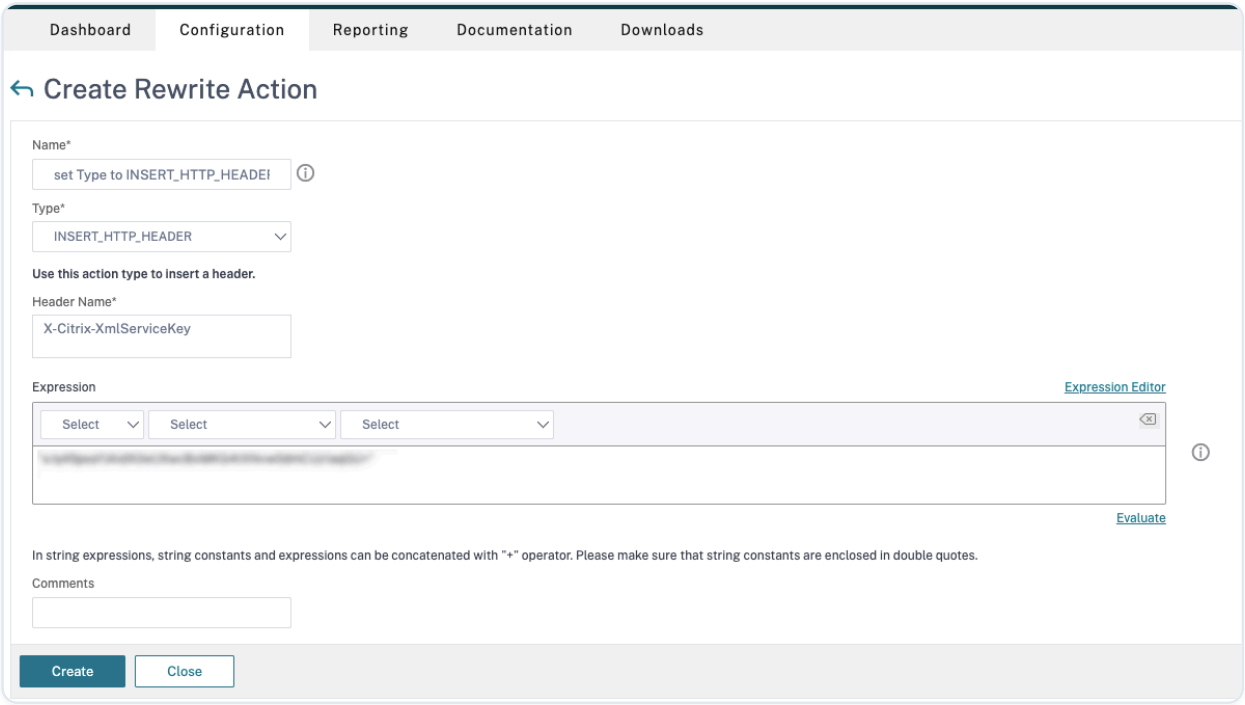
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Add a rewrite action. For details, see Configuring a Rewrite Action.

   a. Go to **AppExpert > Rewrite > Actions**.

   b. Click **Add** to add a new rewrite action. You can name the action as "set Type to INSERT_HTTP_HEADER".

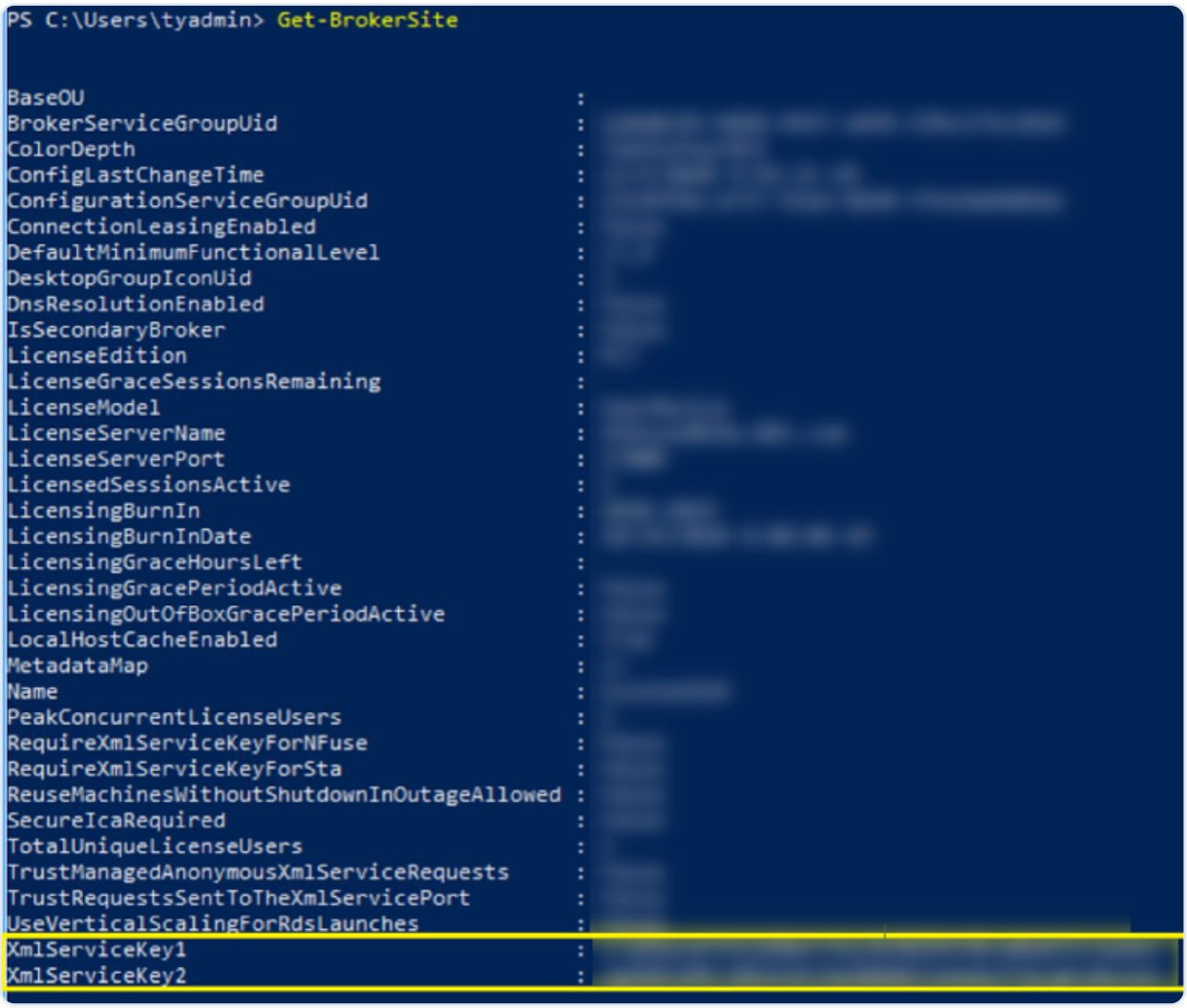


   a. In **Type**, select **INSERT_HTTP_HEADER**.

   b. In **Header Name**, enter X-Citrix-XmlServiceKey.

   c. In **Expression**, add `<XmlServiceKey1 value>` with the quotes. You can copy the XmlServiceKey1 value from your Desktop Delivery Controller™ configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

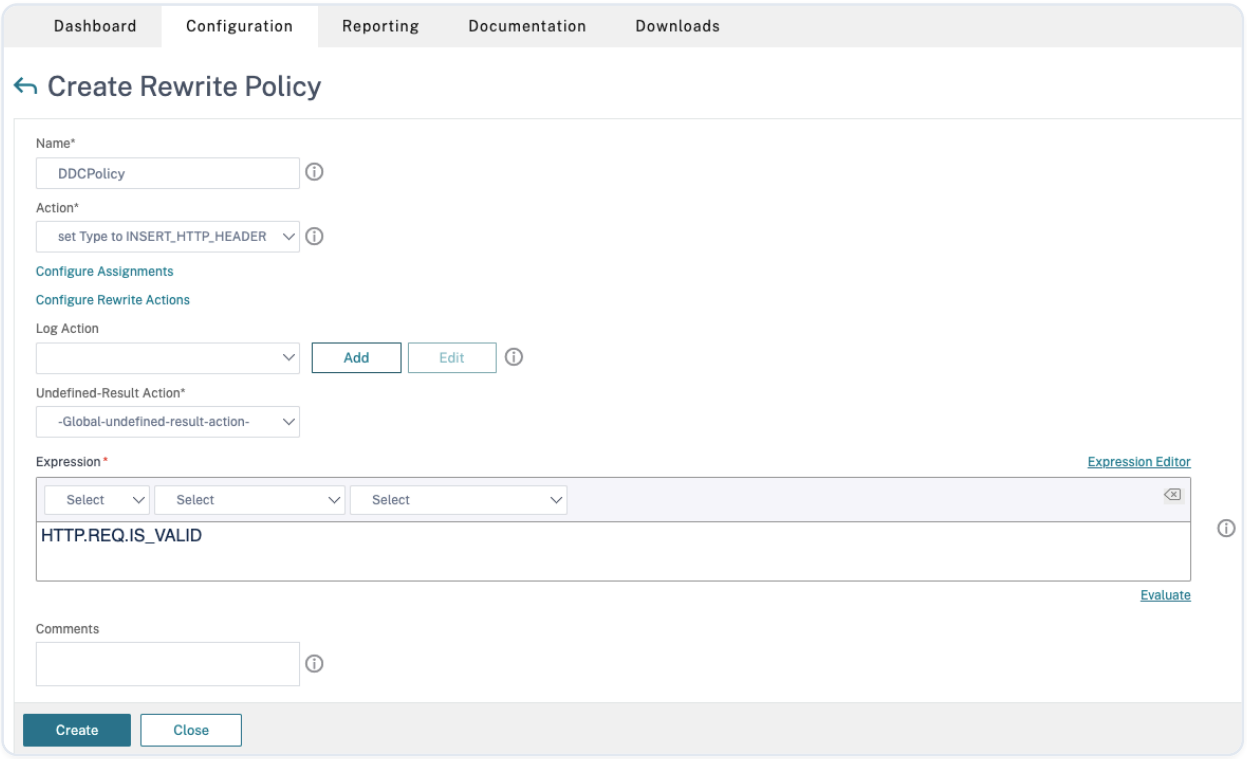


3. Add a rewrite policy. For details, see Configuring a Rewrite Policy.

   a. Go to **AppExpert > Rewrite > Policies**.

   b. Click **Add** to add a new policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. In **Action**, select the action created in the earlier step.

b. In **Expression**, add HTTP.REQ.IS_VALID.

c. Click **OK**.

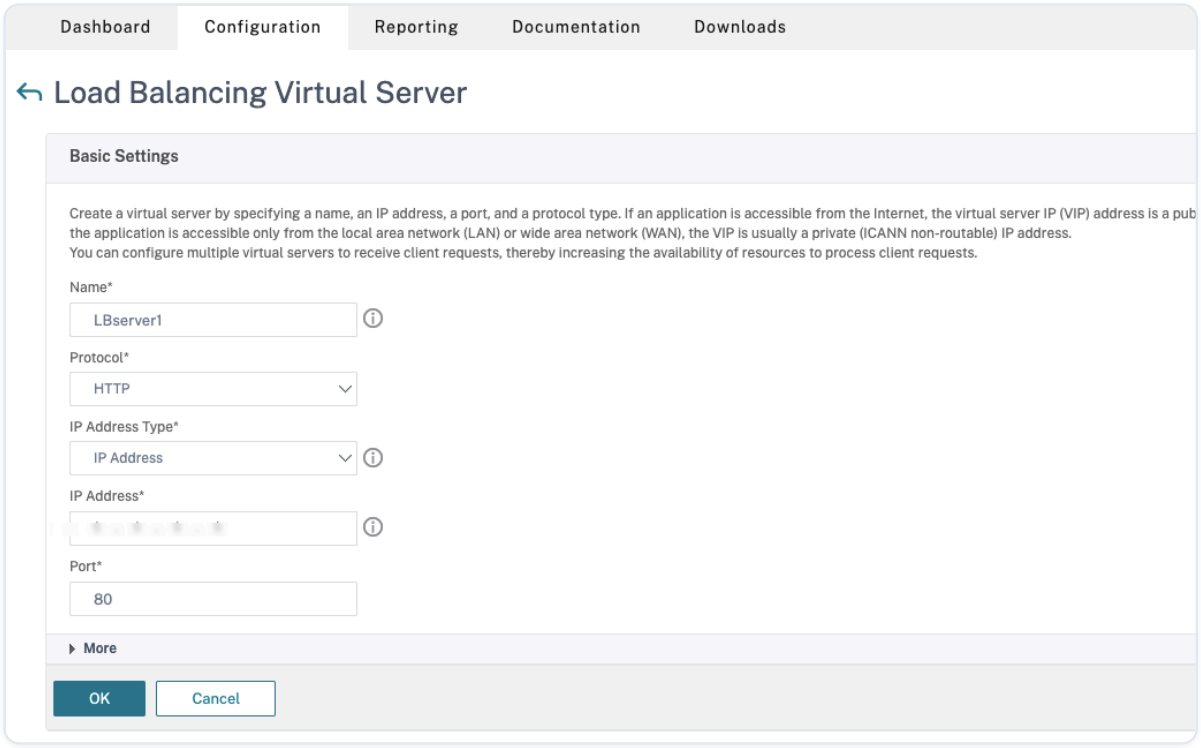
4. Set up load balancing. You must configure one load balancing virtual server per STA server. If not the sessions fail to launch.

   For details, see Set up basic load balancing.

   a. Create a load balancing virtual server.

      - Go to **Traffic Management > Load Balancing > Servers**.
      - In **Virtual Servers** page, click **Add**.

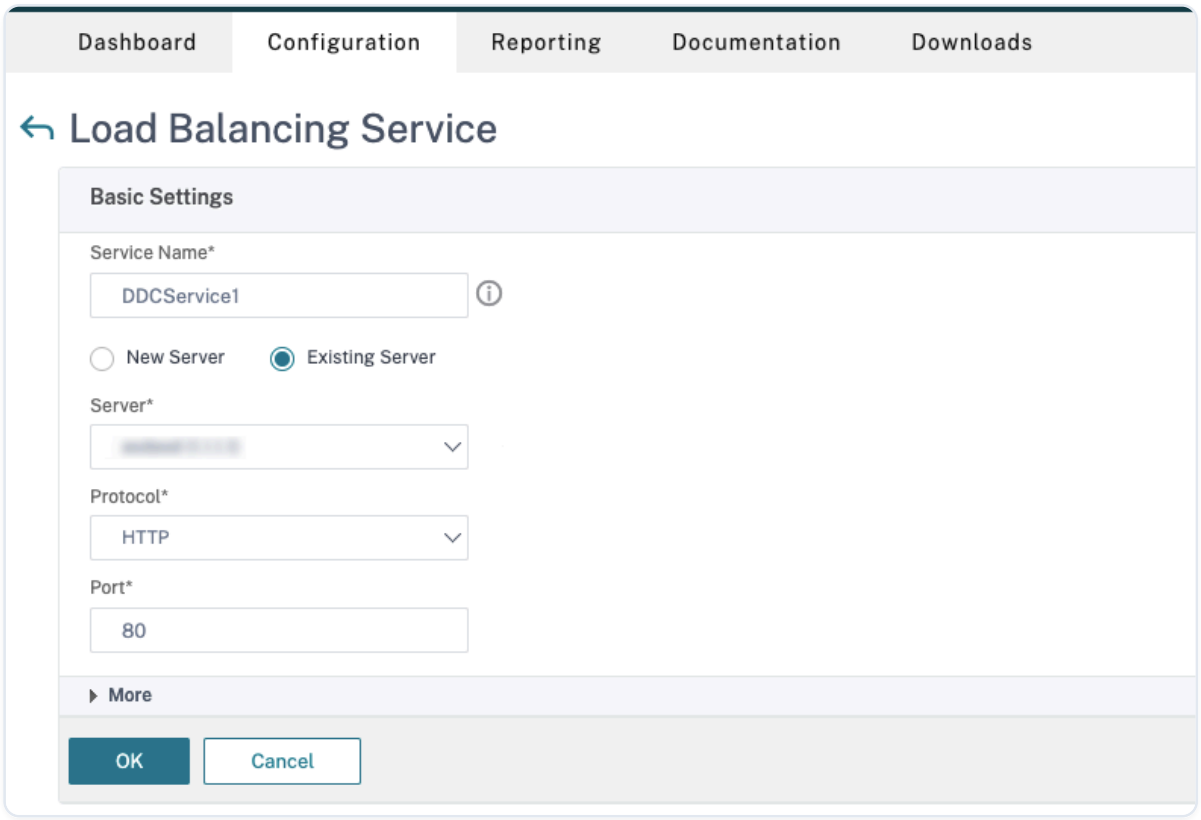
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- In **Protocol**, select **HTTP**.
- Add the load balancing virtual IP address and in **Port** select **80**.
- Click **OK**.

b. Create a load balancing service.

- Go to **Traffic Management > Load Balancing > Services**.

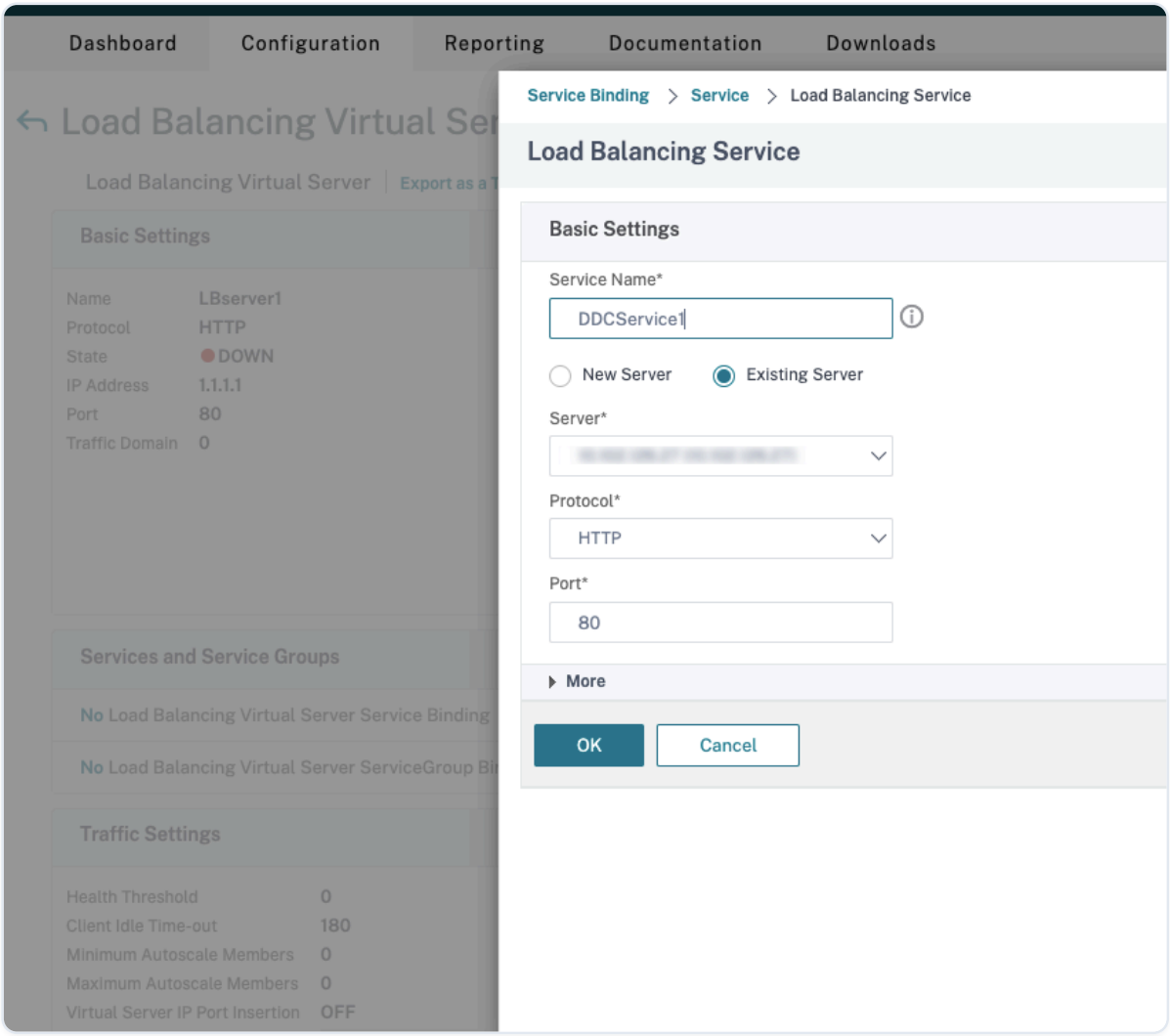


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In **Existing Server**, select the virtual server created in the previous step.
- In **Protocol**, select **HTTP** and in **Port** select **80**.
- Click **OK,** and then click **Done**.

c. Bind the service to the virtual server.

- Select the virtual server created earlier and click **Edit**.
- In **Services and Service Groups**, click **No Load Balancing Virtual Server Service Binding**.

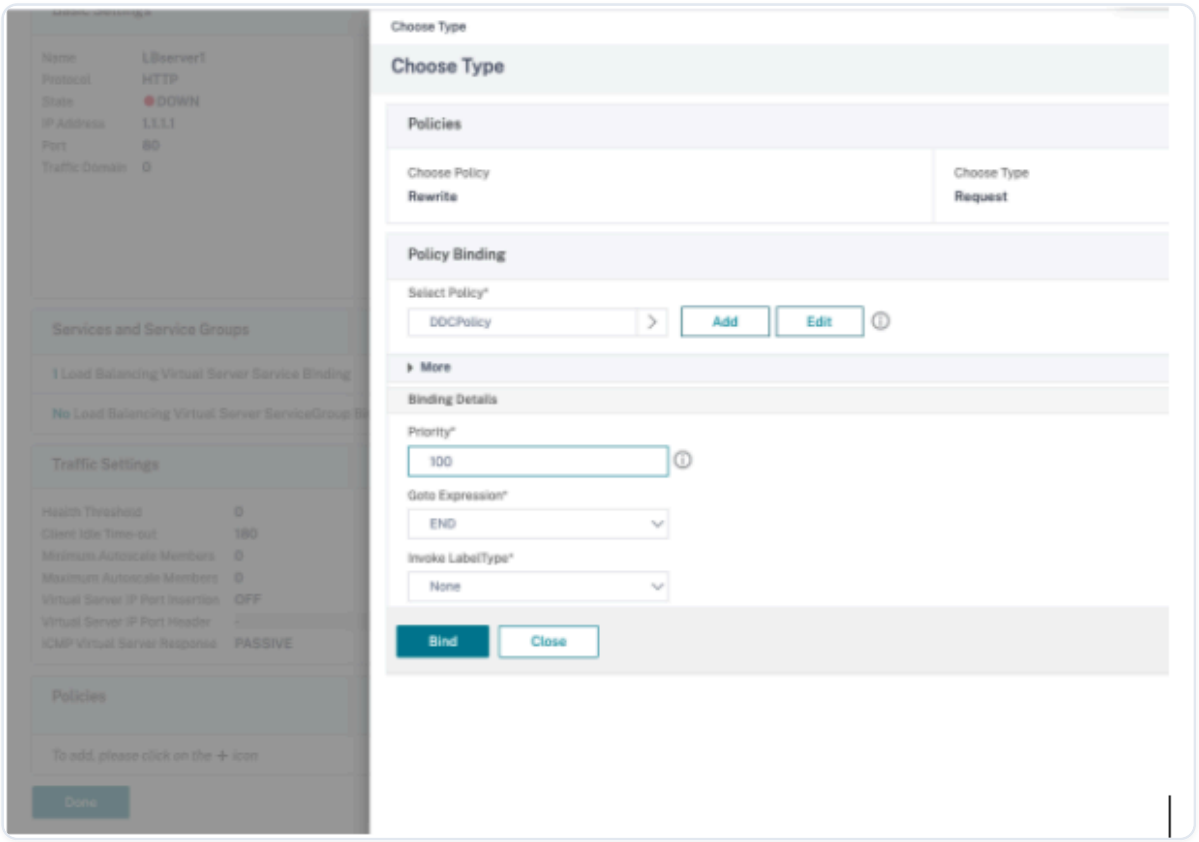


- In **Service Binding**, select Citrix DaaS™ created earlier.
- Click **Bind**.

d. Bind the rewrite policy created earlier to the virtual server.

- Select the virtual server created earlier and click **Edit**.
- In **Advanced Settings**, click **Policies,** and then in **Policies** section click **+**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

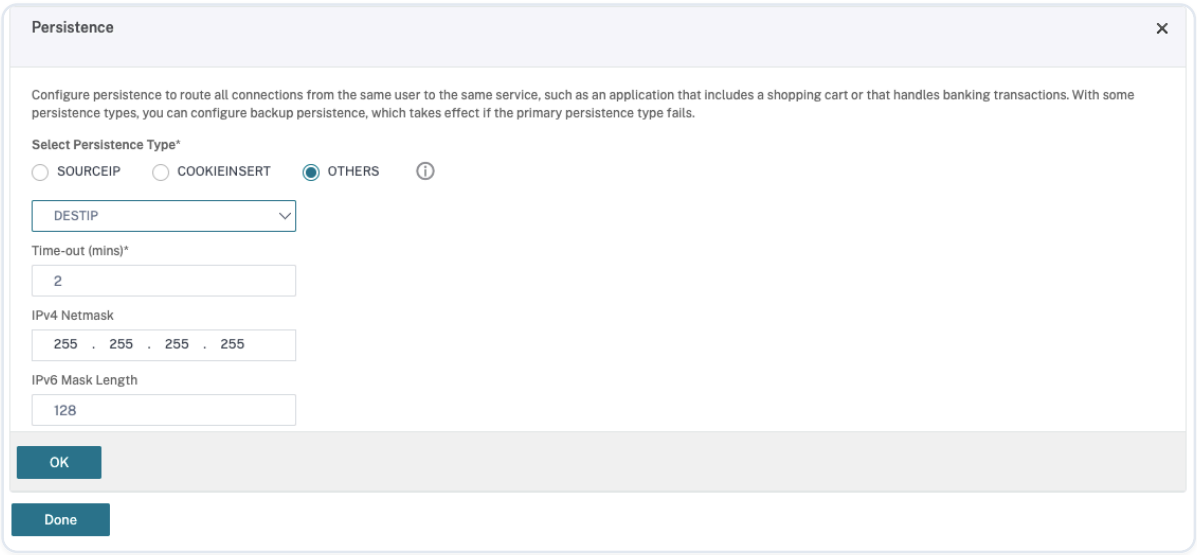


- In **Choose Policy**, select **Rewrite** and in **Choose Type**, select **Request**.
- Click **Continue**.
- In **Select Policy**, select the rewrite policy created earlier.
- Click **Bind**.
- Click **Done**.

e. Set up persistence for the virtual server, if necessary.

- Select the virtual server created earlier and click **Edit**.
- In **Advanced Settings**, click **Persistence**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Select persistence type as **Others**.
- Select **DESTIP** to create persistence sessions based on the IP address of the service selected by the virtual server (the destination IP address)
- In **IPv4 Netmask**, add network mask same as that of the DDC.
- Click **OK**.

f. Repeat these steps for the other virtual server as well.

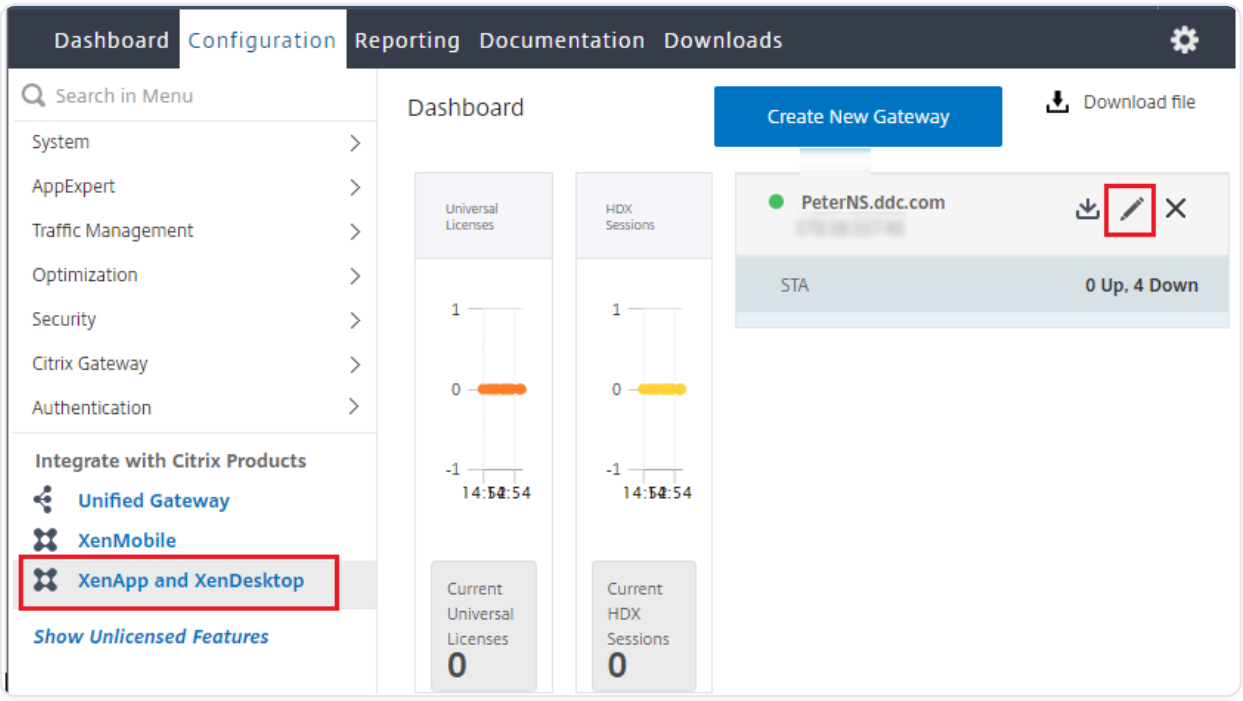
Configuration changes if the Citrix ADC appliance is already configured with Citrix DaaS

If you have already configured the Citrix ADC appliance with Citrix DaaS, then to use the Secure XML feature, you must make the following configuration changes.

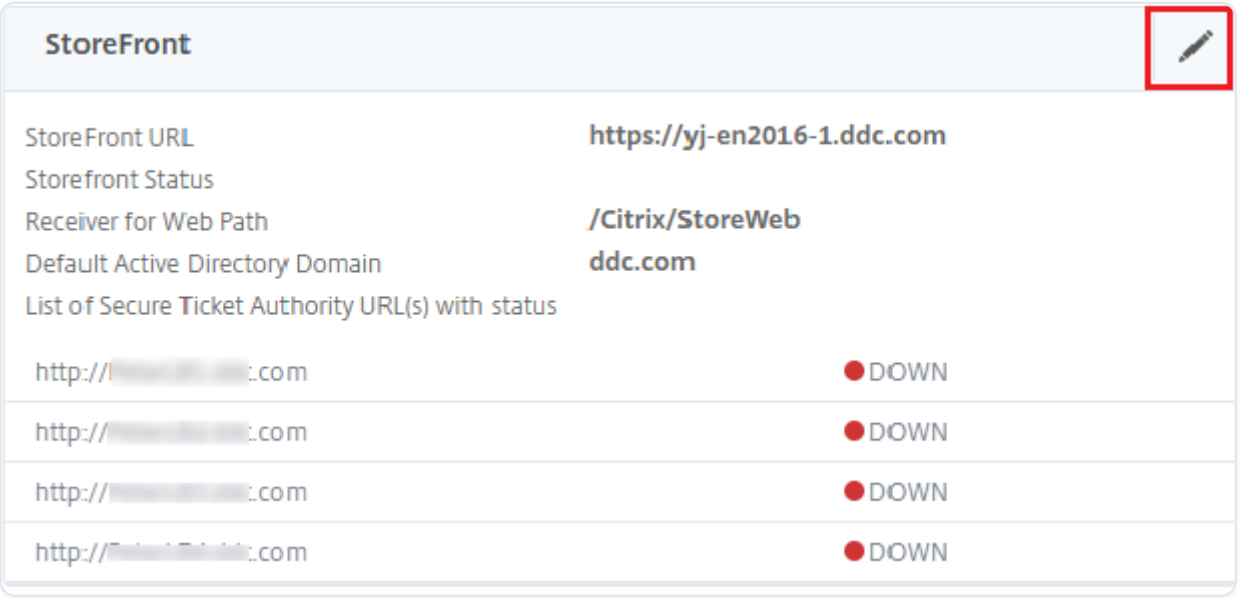
- Before the session launch, change the **Security Ticket Authority URL** of the gateway to use the FQDNs of the load balancing virtual servers.
- Ensure that the `TrustRequestsSentToTheXmlServicePort` parameter is set to False. By default, `TrustRequestsSentToTheXmlServicePort` parameter is set to False. However, if the customer has already configured the Citrix ADC for Citrix DaaS, then the `TrustRequestsSentToTheXmlServicePort` is set to True.

1. In the Citrix ADC GUI, go to **Configuration > Integrate with Citrix Products** and click **XenApp and XenDesktop®**.
2. Select the gateway instance and click the edit icon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



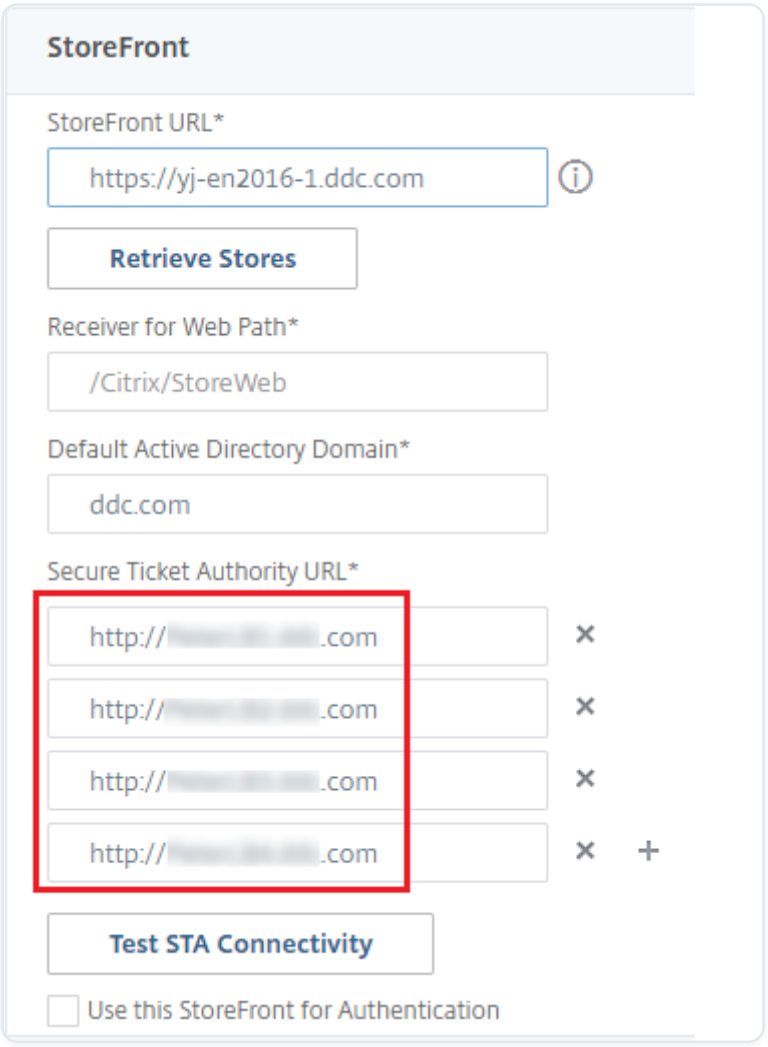
3. In the StoreFront pane, click the edit icon.



4. Add the **Secure Ticket Authority URL**.

   - If the Secure XML feature is enabled, then the STA URL must be the URL of the load balancing service.
   - If the Secure XML feature is disabled, then the STA URL must be the URL of STA (DDC's address) and the TrustRequestsSentToTheXmlServicePort parameter on the DDC must be set to True.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Session resilience settings

Maintaining session activity is critical to providing the best user experience. Losing connectivity due to unreliable networks, highly variable network latency, and range limitations of wireless devices can lead to user frustration. Being able to move quickly between workstations and access the same set of applications each time they log on is a priority for many mobile workers such as healthcare workers in a hospital.

The features described in this article optimize the reliability of sessions, reduce inconvenience, downtime, and loss of productivity; using these features, mobile users can roam quickly and easily between devices.

Session reliability

Session Reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application that they are using until network connectivity resumes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature is especially useful for mobile users with wireless connections. For example, a user with a wireless connection enters a railroad tunnel and momentarily loses connectivity. Ordinarily, the session is disconnected and disappears from the user's screen, and the user has to reconnect to the disconnected session. With Session Reliability, the session remains active on the machine. To indicate that connectivity is lost, the user's display freezes and the cursor changes to a spinning hourglass until connectivity resumes on the other side of the tunnel. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session Reliability reconnects users without reauthentication prompts.

Citrix Workspace™ app users cannot override the Controller setting.

You can use Session Reliability with Transport Layer Security (TLS). TLS encrypts only the data sent between the user device and Citrix Gateway.

Enable and configure Session Reliability with the following policy settings:

- The Session reliability connections policy setting allows or prevents session reliability.
- The Session reliability timeout policy setting has a default of 180 seconds, or three minutes. Although you can extend the amount of time Session Reliability keeps a session open, this feature is designed for user convenience and therefore does not prompt the user for reauthentication. As you extend the amount of time a session is kept open, the chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.
- Incoming session reliability connections use port 2598, unless you change the port number in the Session reliability port number policy setting.
- If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, use the Auto Client Reconnect feature. You can configure the Auto client reconnect authentication policy setting to prompt users to reauthenticate when reconnecting to interrupted sessions.

If you use both Session Reliability and Auto Client Reconnect, the two features work in sequence. Session Reliability closes, or disconnects, the user session after the amount of time you specify in the Session reliability timeout policy setting. After that, the Auto Client Reconnect policy settings take effect, attempting to reconnect the user to the disconnected session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auto Client Reconnect

With the Auto Client Reconnect feature, Citrix Workspace app can detect unintended disconnections of ICA® sessions and reconnect users to the affected sessions automatically. When this feature is enabled on the server, users do not have to reconnect manually to continue working.

For application sessions, Citrix Workspace app attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For desktop sessions, Citrix Workspace app attempts to reconnect to the session for a specified time, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this time is five minutes. To change this period, edit this registry on the user device:

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

Where `seconds` is the number of seconds after which no more attempts are made to reconnect the session.

Enable and configure Auto Client Reconnect with the following policy settings:

- **Auto client reconnect:** Enables or disables automatic reconnection by Citrix Workspace app after a connection has been interrupted.
- **Auto client reconnect authentication:** Enables or disables the requirement for user authentication after automatic reconnection.
- **Auto client reconnect logging:** Enables or disables logging of reconnection events in the event log. Logging is disabled by default. When enabled, the server's System Log captures information about successful and failed automatic reconnection events. Each server stores information about reconnection events in its own system log. The site does not provide a combined log of reconnection events for all servers.

Auto Client Reconnect incorporates an authentication mechanism based on encrypted user credentials. When a user initially logs on, the server encrypts and stores the user credentials in memory, and creates and sends a cookie containing the encryption key to Citrix Workspace app. Citrix Workspace app submits the key to the server for reconnection. The server decrypts the credentials and submits them to Windows Logon for authentication. When cookies expire, users must reauthenticate to reconnect to sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cookies are not used if you enable the auto client reconnection authentication setting. Instead, users are presented with a dialog box to users requesting credentials when Citrix Workspace app attempts to reconnect automatically.

For maximum protection of user credentials and sessions, use encryption for all communication between clients and the Site.

Disable Auto Client Reconnect on Citrix Workspace app for Windows by using the icaclient.adm file. For more information, see the documentation for your Citrix Workspace app for Windows version.

Settings for connections also affect Auto Client Reconnect:

- By default, Auto Client Reconnect is enabled through policy settings at the Site level, as described above. User reauthentication is not required. However, if a server's ICA TCP connection is configured to reset sessions with a broken communication link, automatic reconnection does not occur. Auto Client Reconnect works only if the server disconnects sessions when there is a broken or timed out connection. In this context, the ICA TCP connection refers to a server's virtual port (rather than an actual network connection) that is used for sessions on TCP/IP networks.
- By default, the ICA TCP connection on a server is set to disconnect sessions with broken or timed out connections. Disconnected sessions remain intact in system memory and are available for reconnection by Citrix Workspace app.
- The connection can be configured to reset or log off sessions with broken or timed-out connections. When a session is reset, attempting to reconnect initiates a new session. Rather than restoring a user to the same place in the application in use, the application is restarted.
- If the server is configured to reset sessions, Auto Client Reconnect creates a session. This process requires users to enter their credentials to log on to the server.
- Automatic reconnection can fail if Citrix Workspace app or the plug-in submits incorrect authentication information, which might occur during an attack or the server determines that too much time has elapsed since it detected the broken connection.

ICA Keep-Alive

Enabling the ICA Keep-Alive feature prevents broken connections from being disconnected. When enabled, if the server detects no activity (for example, no clock change, no mouse movement, no screen updates), this feature prevents Remote Desktop Services from disconnecting that session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The server sends keep-alive packets every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

IMPORTANT:

ICA Keep-Alive works only if you are not using Session Reliability. Session Reliability has its own mechanisms to prevent broken connections from being disconnected. Configure ICA Keep-Alive only for connections that do not use Session Reliability.

ICA Keep-Alive settings override keep-alive settings that are configured in the Microsoft Windows Group Policy.

Enable and configure ICA Keep-Alive with the following policy settings:

- **ICA keep alive timeout:** Specifies the interval (1–3600 seconds) used to send ICA keep-alive messages. Do not configure this option if you want your network monitoring software to close inactive connections in environments where broken connections are so infrequent that allowing users to reconnect to sessions is not a concern.

  The default interval is 60 seconds: ICA Keep-Alive packets are sent to user devices every 60 seconds. If a user device does not respond in 60 seconds, the status of the ICA sessions changes to disconnected.
- **ICA keep alives:** Sends or prevents sending ICA keep-alive messages.

Workspace control

Workspace control lets desktops and applications follow a user from one device to another. This ability to roam enables a user to access all desktops or open applications from anywhere simply by logging on, without having to restart the desktops or applications on each device. For example, workspace control can assist healthcare workers in a hospital who need to move quickly among different workstations and access the same set of applications each time they log on. If you configure workspace control options to allow it, these workers can disconnect from multiple applications at one client device and then reconnect to open the same applications at a different client device.

Workspace control affects the following activities:

- **Logging on:** By default, workspace control enables users to reconnect automatically to all running desktops and applications when logging on, bypassing the need to reopen them manually. Through workspace control, users can open disconnected desktops or applications,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

and any that are active on another client device. Disconnecting from a desktop or application leaves it running on the server. If you have roaming users who must keep some desktops or applications running on one client device while they reconnect to a subset of their desktops or applications on another client device, you can configure the logon reconnection behavior to open only the desktops or applications that the user disconnected from previously.

- **Reconnecting:** After logging on to the server, users can reconnect to all of their desktops or applications at any time by clicking Reconnect. By default, Reconnect opens desktops or applications that are disconnected, plus any that are currently running on another client device. You can configure Reconnect to open only those desktops or applications that the user disconnected from previously.
- **Logging off:** For users opening desktops or applications through StoreFront™, you can configure the Log Off command to log the user off from StoreFront and all active sessions together, or log off from StoreFront only.
- **Disconnecting:** Users can disconnect from all running desktops and applications at once, without needing to disconnect from each individually.

Workspace control is available for users who access desktops and applications through a Citrix StoreFront connection, or through the Citrix Workspace app. By default, workspace control is disabled for virtual desktop sessions, but is enabled for hosted applications. Session sharing does not occur by default between published desktops and any published applications running inside those desktops.

User policies, client drive mappings, and printer configurations change appropriately when a user moves to a new client device. Policies and mappings are applied according to the client device where the user is logged on to the session. For example, if a healthcare worker logs off from a client device in the emergency room of a hospital and then logs on to a workstation in the hospital's x-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the x-ray laboratory go into effect at the session startup.

You can customize which printers appear to users when they change locations. You can also control whether users can print to local printers, how much bandwidth is consumed when users connect remotely, and other aspects of their printing experiences.

For information about enabling and configuring workspace control for users, see the StoreFront documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session roaming

NOTE:

The following information guides you to configure session roaming using PowerShell. You can use Studio instead. For more information, see Manage delivery groups.

By default, sessions roam between client devices with the user. When the user launches a session and then moves to another device, the same session is used and applications are simultaneously available on both devices. You can view the applications on multiple devices. The applications follow, regardless of the device or whether current sessions exist. Often, printers and other resources assigned to the application also follow.

While this default behavior offers many advantages, it might not be ideal in all cases. You can prevent session roaming using the PowerShell SDK.

Example 1: A medical professional is using two devices, completing an insurance form on a desktop PC, and looking at patient information on a tablet.

- If session roaming is enabled, both applications appear on both devices (an application launched on one device is visible on all devices in use). This might not meet the security requirements.
- If session roaming is disabled, the patient record does not appear on the desktop PC, and the insurance form does not appear on the tablet.

Example 2: A production manager launches an application on the PC in his office. The device name and location determine which printers and other resources are available for that session. Later in the day, he goes to an office in the next building for a meeting that will require him to use a printer.

- If session roaming is enabled, the production manager would probably be unable to access the printers near the meeting room, because the applications he launched earlier in his office resulted in the assignment of printers and other resources near that location.
- If session roaming is disabled, when he logs on to a different machine (using the same credentials), a new session is started, and nearby printers and resources are available.

Configure session roaming

To configure session roaming, use the following entitlement policy rule cmdlets with the "SessionReconnection" property. Optionally, you can also specify the "LeasingBehavior" property.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For desktop sessions:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

For application sessions:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Where `value` can be one of the following:

- **Always:** Sessions always roam, regardless of the client device and whether the session is connected or disconnected. This is the default value.
- **DisconnectedOnly:** Reconnect only to sessions that are already disconnected; otherwise, launch a new session. (Sessions can roam between client devices by first disconnecting them, or using workspace control to explicitly roam them.) An active connected session from another client device is never used. Instead, a new session is launched.
- **SameEndpointOnly:** A user gets a unique session for each client device that they use. This completely disables roaming. Users can reconnect only to the same device that was previously used in the session.

The "LeasingBehavior" property is described below.

Effects from other setting:

Disabling session roaming is affected by the application limit "Allow only one instance of the application per user" in the application's properties in the Delivery Group.

- If you disable session roaming, then disable the "Allow only one instance ..." application limit.
- If you enable the "Allow only one instance ..." application limit, do not configure either of the two values that allow new sessions on new devices.

Logon interval

If a virtual machine containing a desktop VDA closes before the logon process completes, you can allocate more time to the process. The default for 7.6 and later versions is 180 seconds (the default for 7.0-7.5 is 90 seconds).

On the machine (or the master image used in a machine catalog), set the following registry key:

Key: `HKLM\SOFTWARE\Citrix\PortICA`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Value: `AutoLogonTimeout`
- Type: `DWORD`
- Specify a decimal time in seconds, in the range 0 to 3600.

If you change the master image, roll out the new image to the catalog. For more information, see Change the master image.

This setting applies only to VMs with single-session desktop (workstation) VDAs. Microsoft controls the logon timeout on machines with multi-session server VDAs.

Tags

Introduction

Tags are strings that identify items such as machines, applications, desktops, delivery groups, application groups, and policies. After creating a tag and adding it to an item, you can tailor certain operations to apply only to items that have a specified tag.

- Tailor search displays in Studio.

  For example, to display only applications that have been optimized for testers, create a tag named “test” and then add (apply) it to those applications. You can now filter the search with the tag “test”.

- Publish applications from an application group or specific desktops from a delivery group, considering only a subset of the machines in selected delivery groups. This is called a *tag restriction*.

  With tag restrictions, you can use your existing machines for more than one publishing task, saving the costs associated with deploying and managing more machines. A tag restriction can be thought of as subdividing (or partitioning) the machines in a delivery group. Its functionality is similar, but not identical, to worker groups in XenApp releases earlier than 7.x.

  Using an application group or desktops with a tag restriction can be helpful when isolating and troubleshooting a subset of machines in a delivery group.

  Details and examples of using a tag restriction are described later in this article.

- Schedule periodic restarts for a subset of machines in a delivery group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using a tag restriction for machines enables you to use new PowerShell cmdlets to configure multiple restart schedules for subsets of machines in a delivery group. For examples and details, see Manage delivery groups.

- Tailor the application (assignment) of Citrix® policies to machines in delivery groups, delivery group types, or OUs that have (or don't have) a specified tag.

  For example, if you want to apply a Citrix policy only to the more powerful workstations, add a tag named “high power” to those machines. Then, on the **Assign Policy** page of the Create Policy wizard, select that tag and the **Enable** check box. You can also add a tag to a delivery group and then apply a Citrix policy to that group. For details, see Create policies.

You can apply tags to:

- Machines
- Applications
- Machine catalogs
- Delivery groups
- Application groups

You can configure a tag restriction when creating or editing the following in Studio:

- A desktop in a shared delivery group
- An application group

IMPORTANT:

A tag can be explicitly applied to a machine or can be explicitly applied at the machine catalog or delivery group level. When a tag is applied at the machine catalog or delivery group level, all machines within that catalog or delivery group implicitly inherit the tag. These inherited tags cannot be removed at the machine level. To remove the tag effect, the tag must be removed from the machine catalog or delivery group level.

Tag restrictions for a desktop or an application group

A tag restriction involves several steps:

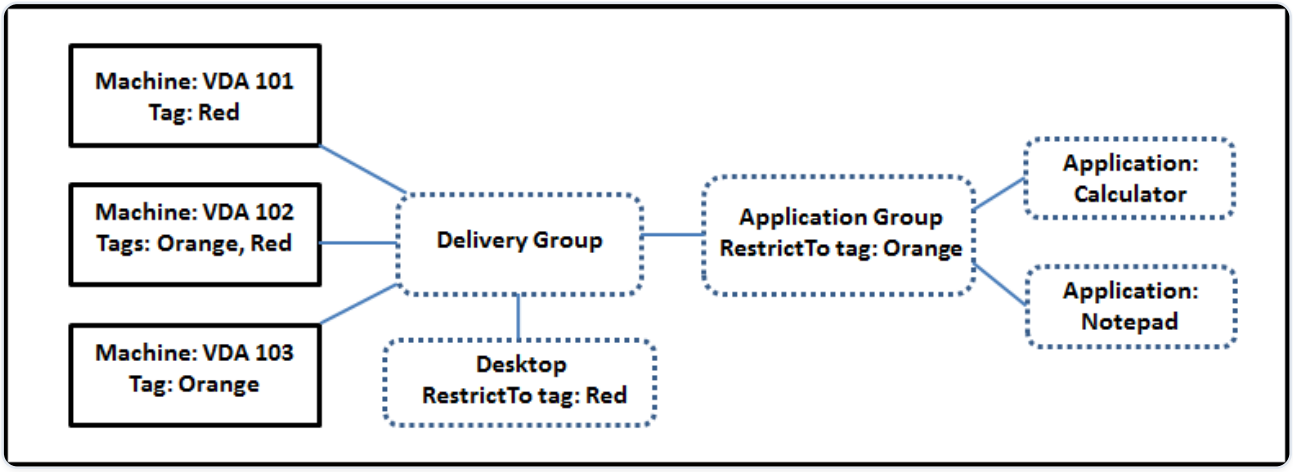
- Create the tag and then add (apply) it to machines.
- Create or edit a group with the tag restriction (in other words, restrict launches to machines with tag *x*).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A tag restriction extends the Controller's machine selection process. The Controller selects a machine from an associated delivery group, subject to access policy, configured user lists, zone preference, and launch readiness, plus the tag restriction (if present). For applications, the Controller falls back to other delivery groups in priority order, applying the same machine selection rules for each considered delivery group.

Example 1: Simple layout

This example introduces a simple layout that uses tag restrictions to limit which machines are considered for certain desktop and application launches. There is one shared delivery group, one published desktop, and one application group configured with two applications.



- Tags have been added to each of the three machines (VDA 101-103).
- The desktop in the delivery group was created with a tag restriction named `Red`. So, that desktop can be launched only on machines in that delivery group that have the tag `Red`: VDA 101 and 102.
- The application group was created with the `Orange` tag restriction. So, each of its applications (`Calculator` and `Notepad`) can be launched only on machines in that delivery group that have the tag `Orange`: VDA 102 and 103.

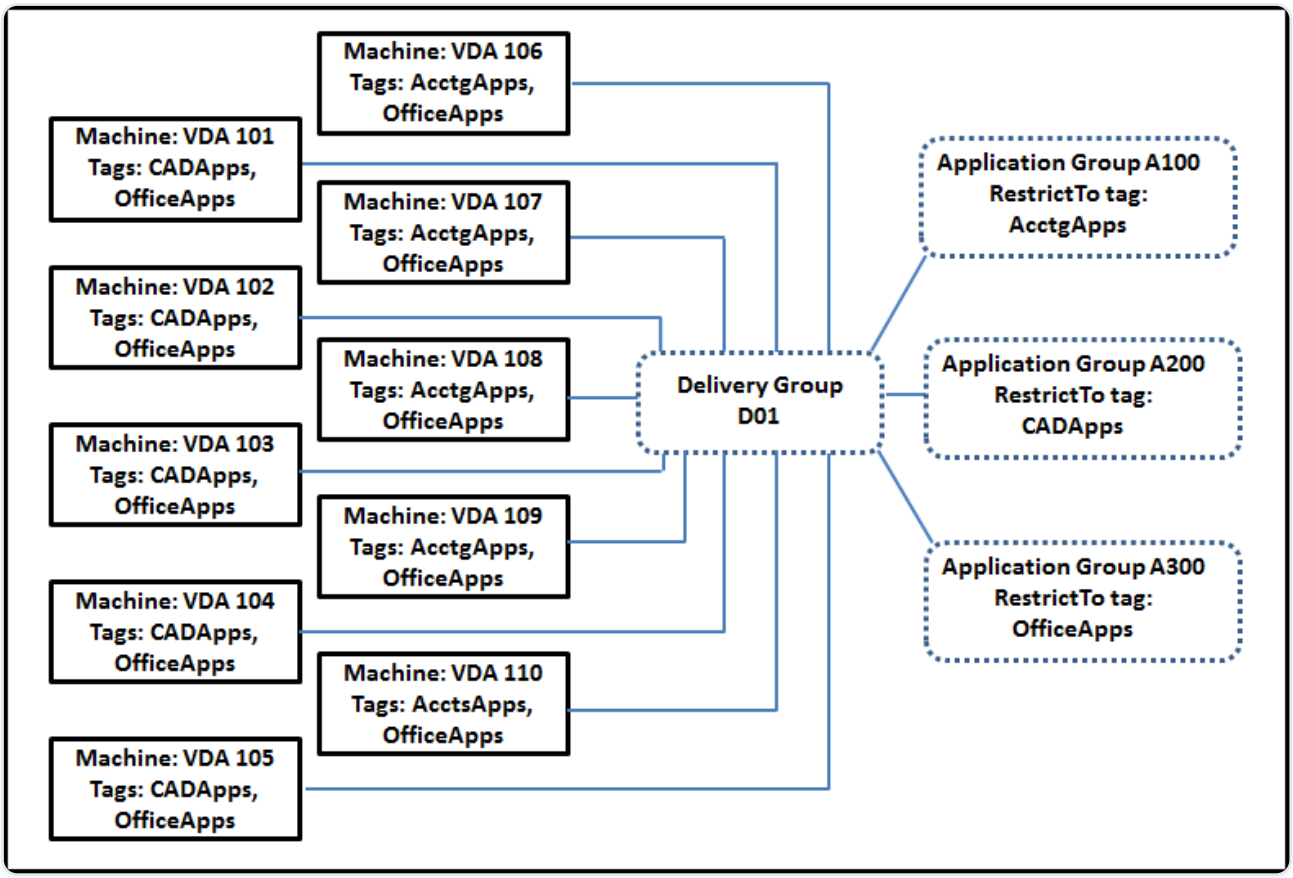
Machine VDA 102 has both tags (`Red` and `Orange`), so it can be considered for launching the applications and the desktop.

Example 2: More complex layout

This example contains several application groups that were created with tag restrictions. This results in the ability to deliver more applications with fewer machines than would otherwise be needed if you used only delivery groups.

How to configure example 2 shows the steps used to create and apply the tags, and then configure the tag restrictions in this example.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



This example uses 10 machines (VDA 101-110), one delivery group (`D01`), and three application groups (`A100` , `A200` , `A300`). By applying tags to each machine and then specifying tag restrictions when creating each application group:

- Accounting users in the group can access the apps they need on five machines (VDA 101–105)
- CAD designers in the group can access the apps they need on five machines (VDA 106-110)
- Users in the group who need Office applications can access the Office apps on 10 machines (VDA 101-110)

Only 10 machines are used, with only one delivery group. Using delivery groups alone (without application groups) would require twice as many machines, because a machine can belong to only one delivery group.

Manage tags and tag restrictions

Tags are created, added (applied), edited, and deleted from selected items through the **Manage Tags** action in Studio.

(Exception: Tags used for policy assignments are created, edited, and deleted through the **Manage Tags** action. However, you apply (assign) tags when you create the policy. See Create policies for details.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tag restrictions are configured when you create or edit desktops in delivery groups, and when you create and edit application groups.

Use the Manage Tags feature

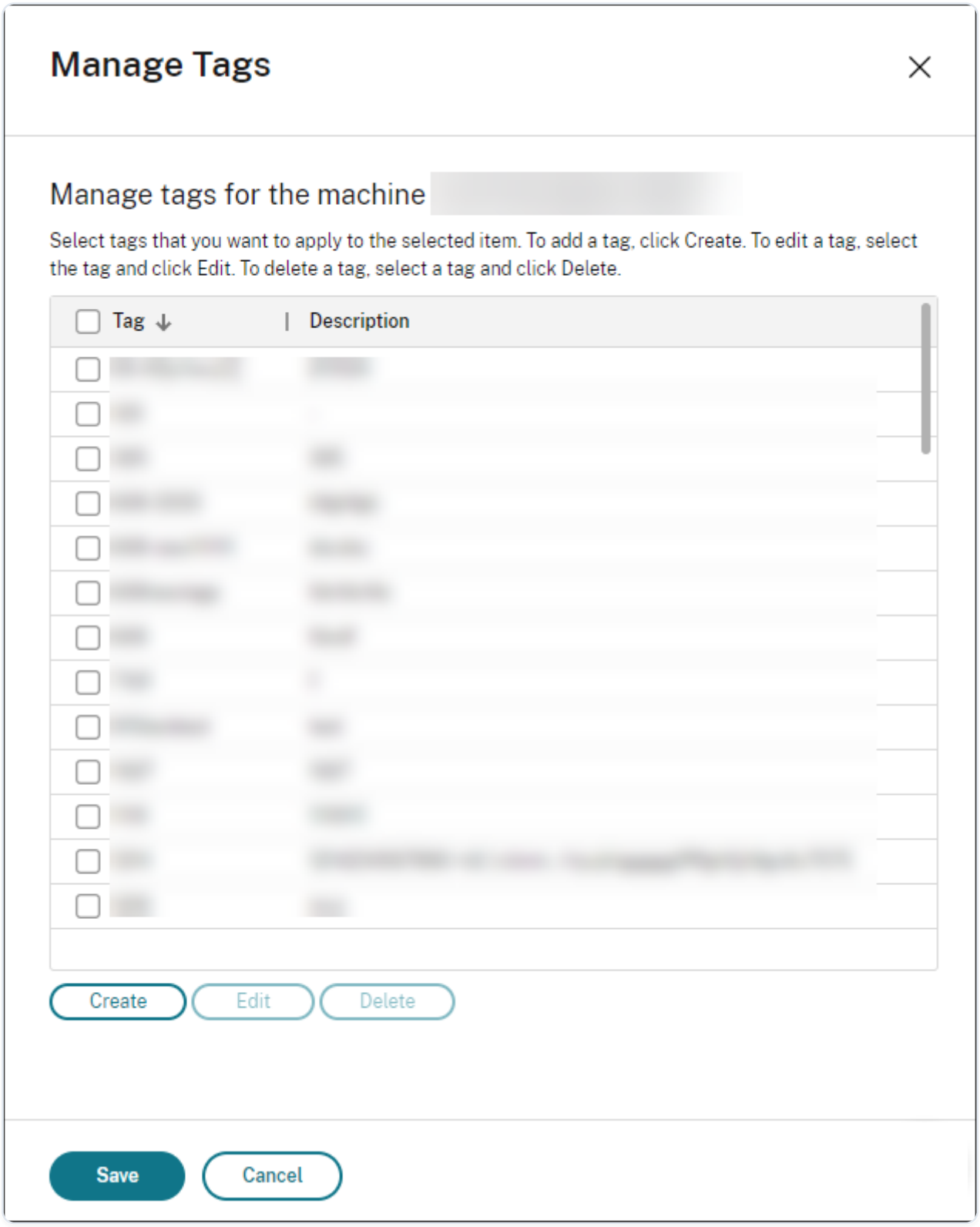
From Studio, select the items to which you want to apply a tag. The items include:

- One or more machines
- One or more applications
- A desktop, a delivery group, or an application group
- A machine catalog

Then select **Manage Tags** in the action bar. The **Manage Tags** dialog box lists all existing tags, not just those for the items you selected.

- An enabled check box indicates that the tag has already been added to the selected items. (In the screen capture below, the selected machine has a tag named “Tag1” applied.)
- If you select more than one item, a check box containing a hyphen indicates that some but not all selected items have that tag added.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following actions are available from the **Manage Tags** dialog box. Review Cautions when working with tags.

- **To create a tag:**

  Select **Create.** Enter a name and description. Tag names must be unique and are not case-sensitive. Then select **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Creating a tag does not automatically apply it to any items you have selected. Use the check boxes to apply the tag.

- **To add (apply) one or more tags:**

  Enable the check box next to the tag name. A check box containing a hyphen indicates that some, but not all selected items already have the tag applied. When you select multiple items and a tag's check box has a hyphen, changing it to a check mark affects all selected machines.

  If you attempt to add a tag to machines, and that tag is used as a restriction in an application group, you are warned that the action can make those machines available for launch. If that's what you intend, proceed.

- **To remove one or more tags:**

  Clear the check box next to the tag name. A check box containing a hyphen indicates that some, but not all selected items already have the tag applied. When you select multiple items and a tag's check box has a hyphen, clearing the check box removes the tag from all selected machines.

  If you try to remove a tag restriction from a machine, you're warned that the action can affect the machines considered for launch. If that's what you intend, proceed.

- **To edit a tag:**

  Select a tag and then select **Edit**. Enter a new name, description, or both. You can edit only one tag at a time.

- **To delete one or more tags:**

  Select the tags and then select **Delete**. The **Delete Tag** dialog box indicates how many items currently use the selected tags (for example "2 machines"). Select an item to display more information (for example, the names of the two machines that have the tag applied). Confirm whether you want to delete the tags.

  You cannot delete a tag that is used as a restriction. First, edit the application group and remove the tag restriction or select a different tag.

When you're done in the **Manage Tags** dialog box, select **Save**.

To see if a machine has any tags applied: Select **Delivery Groups** in the left pane. Select a delivery group then select **View Machines** in the action bar. Select a machine and then select the **Tags** tab on the **Details** pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage tag restrictions

Configuring a tag restriction is a multi-step process: You first create the tag and add/apply it to machines. Then, you add the restriction to the application group or the desktop.

- **Create and apply the tag:**

  Create the tag and then add (apply) it to the machines that the tag restriction will affect, using **Manage Tags** actions.

- **To add a tag restriction to an application group:**

  Create or edit the application group. On the **Delivery Groups** page, select **Restrict launches to machines with the tag** and then select the tag from the list.

- **To change or remove the tag restriction on an application group:**

  Edit the group. On the **Delivery Groups** page, either select a different tag from the list or remove the tag restriction entirely by clearing **Restrict launches to machines with the tag**.

- **To add a tag restriction to a desktop:**

  Create or edit a delivery group. Select **Add** or **Edit** on the **Desktops** page. In the **Add Desktop** dialog box, select **Restrict launches to machines with the tag** and then select the tag from the menu.

- **To change or remove the tag restriction on a delivery group:**

  Edit the group. On the **Desktops** page, select **Edit**. In the dialog box, either select a different tag from the list or remove the tag restriction entirely by clearing **Restrict launches to machines with the tag**.

Cautions when working with tags

A tag applied to an item can be used for different purposes. Keep in mind that adding, removing, and deleting a tag can have unintended effects. You can use a tag to sort machine displays when using search in Studio. You can use the same tag as a restriction when configuring an application group or a desktop. That action limits launch consideration to only machines in specified delivery groups that have that tag.

If you add a tag to machines after that tag is configured as a desktop or application group tag restriction, you are warned that might make the machines available for launching more applications or desktops. If that's what you intend, proceed. If not, cancel the operation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, let's say you create an application group with the `Red` tag restriction. Later, you add several other machines in the same delivery groups used by that application group. If you then try to add the `Red` tag to those machines, you see a message similar to: "The tag `Red` is used as a restriction on the following application groups. Adding this tag might make the selected machines available to launch applications in this application group." You can then confirm or cancel adding that tag to those additional machines.

Similarly, when a tag is used in an application group to restrict launches, you cannot delete the tag until you edit the group and remove it as a restriction. (If you were allowed to delete that tag, it might result in allowing applications to launch on all machines in the delivery groups associated with the application group.) The same prohibition against deleting a tag applies if the tag is being used as a restriction for desktop launches. After you edit the application group or desktops in the delivery group to remove that tag restriction, you can delete the tag.

All machines might not have the same sets of applications. A user can belong to more than one application group, each with a different tag restriction and different or overlapping sets of machines from delivery groups. The following table lists how machine considerations are decided.

WHEN AN APPLICATION HAS BEEN ADDED TO	THESE MACHINES IN THE SELECTED DELIVERY GROUPS ARE CONSIDERED FOR LAUNCH
One application group with no tag restriction	Any machine.
One application group with tag restriction A	Machines that have tag A applied.
Two application groups, one with tag restriction A and the other with tag restriction B	Machines that have tag A and tag B. If none is available, then machines that have tag A or tag B.
Two application groups, one with tag restriction A and the other with no tag restriction	Machines that have tag A. If none is available, then any machine.

If you used a tag restriction in a machine restart schedule, any changes you make that affect tag applications or restrictions affect the next machine restart cycle. It does not affect any restart cycles that are in progress while the changes are being made.

How to configure example 2

The following sequence shows the steps to create and apply tags, and then configure tag restrictions for the application groups illustrated in the earlier second example.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDAs and applications have already been installed on the machines and the delivery group has been created.

Create and apply tags to the machines:

1. From Studio, select **Delivery Groups** in the left pane. Select delivery group `D01` and then select **View Machines** in the action bar.
2. Select machines VDA 101-105 and then select **Manage Tags** in the action bar.
3. In the **Manage Tags** dialog box, select **Create**. Create a tag named `CADApps`. Select **OK**.
4. Select **Create** again and create a tag named `OfficeApps`. Select **OK**.
5. Add (apply) the newly created tags to the selected machines by enabling the check boxes next to each tag's name (`CADApps` and `OfficeApps`). Then close the dialog box.
6. Select delivery group `D01`. Select **View Machines** in the action bar.
7. Select machines VDA 106-110 and then select **Manage Tags** in the action bar.
8. In the **Manage Tags** dialog box, select **Create**. Create a tag named `AcctgApps`. Select **OK**.
9. Apply the newly created `AcctgApps` tag and the `OfficeApps` tag to the selected machines by selecting the check boxes next to each tag's name. Then close the dialog box.

Create the application groups with tag restrictions.

1. From Studio, select **Applications** in the left pane.
2. Select **Create Application Group** in the action bar. The wizard launches.
3. On the **Delivery Groups** page, select delivery group `D01`. Select **Restrict launches to machines with tag** and then select the `AcctgApps` tag from the list.
4. Complete the wizard, specifying the accounting users and the accounting applications. (When adding the application, choose the **From Start menu** source, which searches for the application on the machines that have the `AcctgApps` tag.) On the **Summary** page, name the group `A100`.
5. Repeat the preceding steps to create application group `A200`, specifying machines that have the `CADApps` tag, plus the appropriate users and applications.
6. Repeat steps to create application group `A300`, specifying machines that have the `OfficeApps` tag, plus the appropriate users and applications.

Apply tags to machine catalogs

You can use Studio or PowerShell to apply tags to machine catalogs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Using the management interface is described in Manage tags. Catalog displays do not indicate whether tags are applied.
- To use PowerShell, see Use PowerShell to apply tags to catalogs.

Here is an example of using tags with catalogs:

- A delivery group contains machines from several catalogs, but you want an operation (such as a restart schedule) to affect only the machines in a specific catalog. Applying a tag to that catalog accomplishes that goal.

Use PowerShell to apply tags to catalogs

The following PowerShell cmdlets are available:

- You can pass catalog objects to cmdlets such as `Add-BrokerTag` and `Remove-BrokerTag`.
- `Get-BrokerTagUsage` shows how many catalogs contain tags.
- `Get-BrokerCatalog` has a property named `Tags`.

For example, the following cmdlets add a previously created tag named `fy2018` to the catalog named `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`.

See the PowerShell cmdlet help for guidance and syntax.

Auto tags

Using auto tags, you can define rules for automatic addition and removal of tags on machines, application groups, applications, desktop groups, or desktops. The tags are also automatically removed if they do not meet the defined rules. This enhancement eliminates the need to maintain different scripts that run periodically for environment optimization.

Use cases

With auto-tagging, you can implement rules relevant to your business drivers, such as reducing costs, optimizing the infrastructure, and driving consumption. The following are some of the use cases:

- **Reclaim unused VDIs** - To release the dedicated workloads that have not been used for more than a pre-configured number of days to the available pool.
- **Remove App clutter** - To reduce application clutter by identifying the applications that have not been used for more than a pre-configured number of days.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **DGs with less than X functional level** - To find delivery groups with less than a specific functional level.
- **Inactive users** - To reclaim resources of users who have not logged on for more than a pre-configured number of days.

NOTE:

The tag attached to a machine that has not been used for more than 30 days is removed from that machine the next time it runs if a user logs in that machine after 30 days.

PowerShell commands

You can create autotags using PowerShell commands. After an autotag rule is created, it is evaluated at a frequency of 3600 seconds. For more information, see New-BrokerAutoTagRule.

The parameters of `New-BrokerAutoTagRule` are:

- Name: Generic name for the rule
- Object type: Machine
- Rule text : The filter to define the rule.
- Tag Uid: The tag id that you want to associate with.

Examples

1. To tag dedicated VDIs that have not been used for more than 30 days:

   ```
   New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText
   “-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne
   `”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime
   -eq `$null ) }” -TagUid 123
   ```

   After the rule is configured, the machines with the tag **unused-VDI** are released.

2. To tag delivery groups with less than X functional level (using **L7_20** as the threshold functional level):

   ```
   New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup'
   -RuleText " -Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid
   143
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. To tag user visible apps published without a folder:

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application'
-RuleText "-Enabled $true -Filter { ClientFolder -eq $null } " -TagUid
153`
```

More information

Blog post: How to assign desktops to specific servers.

Tasks in Task Center

Task Center provides a centralized view of scheduled and recurring tasks in Citrix DaaS™. You can track task status in real time and manage tasks from a single location in Studio.

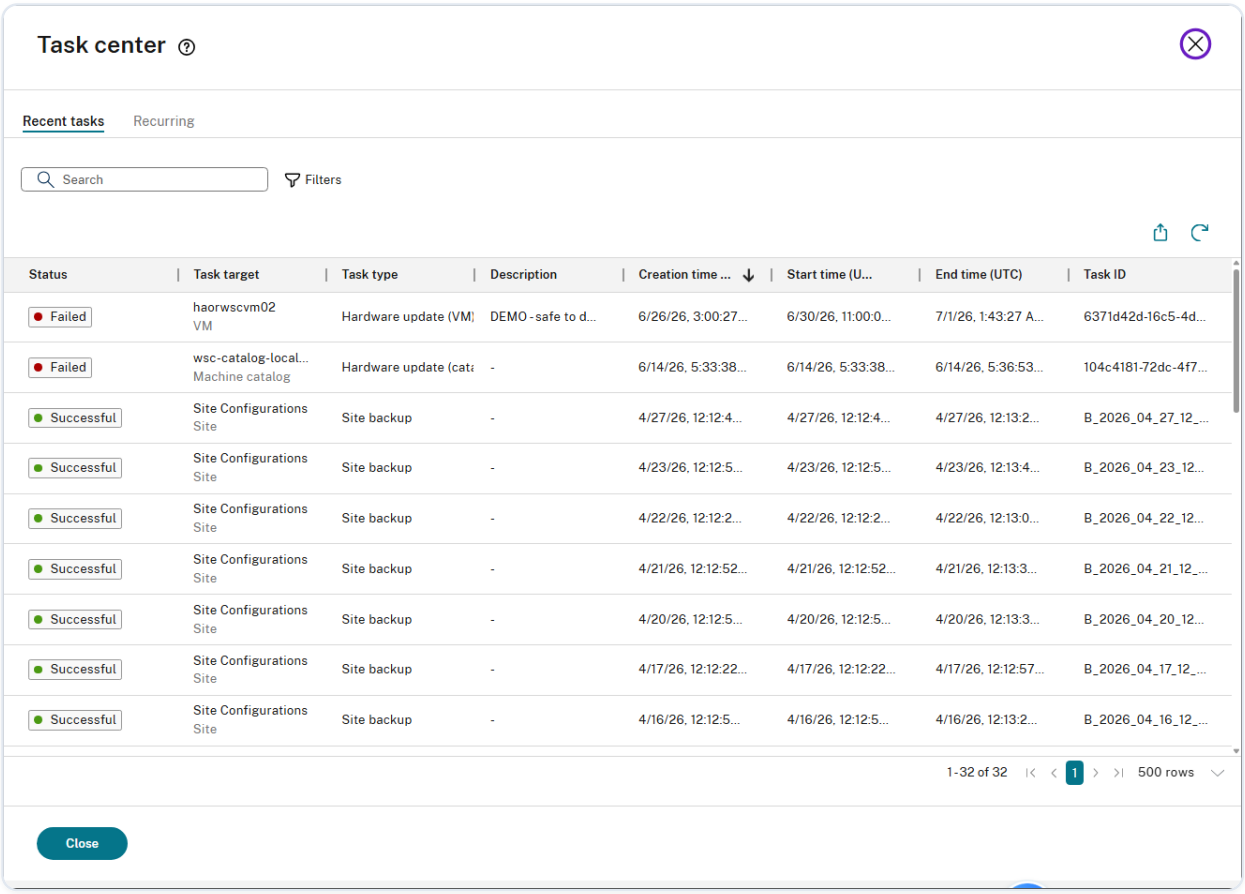
Access Task Center

1. Open the Studio console.
2. In the upper-right corner, select the **Calendar** icon.

   The Task Center panel opens.

   - The **Recent tasks** tab shows individual task runs from the past 90 days.
   - The **Recurring** tab shows tasks scheduled to run periodically or in the future.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



View and manage recent tasks

In the **Recent** tab, you can:

- Search and filter tasks using the search bar.
- Track real-time task status.
- Perform actions on tasks, such as cancel or rerun.

Each task entry displays the following details:

FIELD	DESCRIPTION
Status	Current state of the task: Successful, Canceled, In progress, or Failed
Task Target	Resource the task applies to
Task Type	Type of operation (for example, OS disk reset, VM backup)
Description	Summary of the operation

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD	DESCRIPTION
Task ID	Unique identifier for tracking

View and manage recurring tasks

In the **Recurring** tab, you can:

- Search and filter recurring schedules using the search bar.
- Track the state of recurring schedules in real time.
- Perform actions on recurring schedules, such as edit or delete.

Each recurring entry displays the following details:

FIELD	DESCRIPTION
State	Current state of the recurring schedule: Enabled or Disabled
Task Target	Resource the recurring schedule applies to
Task Type	Type of operation, such as site backup or restart schedule
Schedule Name	Name of the recurring schedule
Description	Summary of the operation
Frequency	Frequency of the recurring schedule: Daily, Weekly, or Monthly

Supported task types

- Site backup
- Restart schedule

Citrix Troubleshoot Connection

The Citrix Troubleshoot Connection feature is designed to empower end-users to effectively self-troubleshoot potential desktop or application launch failures. This enhancement aims to provide

© 1997–2026 Citrix Systems, Inc. All rights reserved.

users with clear diagnostics, potential recommendations, and the ability to run fixes with a simple click.

Overview

Citrix now delivers more granular and enhanced error messages to help users clearly understand the root cause of launch failures. The Troubleshoot Connection feature performs real-time analysis of reachability challenges to the Virtual Delivery Agent (VDA) during the launch process. It then presents user-friendly error messages and recommendations, enabling users to either resolve the issue directly or gather logs for a support ticket if needed.

Connection paths analyzed

The feature diagnoses potential virtual app and desktop launch issues across critical connection points, including:

- Network connectivity from the Client to the Gateway.
- Gateway to StoreFront server connection.
- StoreFront server to Broker connection.
- Broker to VDA connection.

Enhanced error messages and diagnostics

In the event of launch failures, Citrix now displays clear, user-friendly error messages that pinpoint specific connection issues, such as network errors, server unavailability, or VDA failures. For administrators, detailed error codes are provided in the logs, categorized into server-side and client-side errors, serving as valuable references for deeper investigation.

Self-recovery and remediation actions

The Citrix Troubleshoot Connection feature includes steps that users can take to automatically recover from common issues, thereby minimizing the need for support intervention. Following are the potential problems that can be resolved with guided remediation:

- Restart VDA
- Restart Citrix Workspace app (CWA) - Re-Login to CWA
- Refresh the resource list
- Refresh the app and try
- Reconfigure the store

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Upgrade CWA
- Reinstall CWA
- Check the network
- Wait And retry

System requirements

To use the Troubleshoot Connection feature, have the following Citrix Workspace app versions:

- **Citrix Workspace app for Mac:** Version 2505 and later
- **Citrix Workspace app for Windows:** Version 2507 and later
- **Citrix Workspace app for iOS:** Version 2509 and later
- **Citrix Workspace app for Android:** Version 2509 and later

How to use

The Troubleshoot Connection feature is enabled by default for Citrix DaaS environments. Granular and enhanced error messages, along with remediation recommendations, are provided for both browser-launched sessions and sessions launched directly through the native Citrix Workspace app.

Important considerations

While the feature offers robust self-service capabilities, it's important to note the following:

- The "Restart VDA" remediation action does not support sessions launched through a hybrid launch mode (that is, downloading an ICA file from a browser and then launching it with the native Citrix Workspace app).

Error codes

The error codes are split between server side errors and client side errors. Following are the tables with error codes.

Common server-side errors

ERROR ID	DESCRIPTION	RECOMMENDATION
`ResourceNotFound`	The resource was removed by your administrator.	For an up-to-date list of available apps and desktops, either refresh Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR ID	DESCRIPTION	RECOMMENDATION
		Workspace app or log out and back in.
`WorkstationInMaintenance`	The desktop is under planned maintenance.	Wait until the maintenance is complete, then try again.
`UnavailableDesktop`	There are no desktops available to connect to.	Wait a few minutes, then try again. If the issue persists, contact your system administrator.
`UnavailableAppProtectedDesktop`	App Protection required to open protected resources.	Upgrade to a Citrix Workspace app version with App Protection, or contact your system administrator for assistance.
`NotLicensed`	Unable to launch the resource because the server is missing the appropriate license.	Contact your system administrator for assistance.
`NoMoreActiveSessions`	Unable to launch the resource because there are no available session slots.	Wait a few minutes, then try again. If the issue persists, contact your system administrator.
`GeneralAppLaunchError`	An unknown error occurred while trying to open the resource.	Contact your system administrator for assistance.
`ResourceDisabled`	Your administrator has disabled the resource.	For an up-to-date list of available apps and desktops, either refresh Citrix Workspace app or log out and back in.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app for Windows

ERROR ID	DESCRIPTION	RECOMMENDATION
`CertificateError`	An error occurred with the server certificate.	Contact your system administrator for assistance.
`PassthroughClientError`	There is already an active session.	Contact your system administrator for assistance.
`IcaFileRetrieveError`	An error occurred while trying to retrieve the ICA file.	Contact your system administrator for assistance.
`IcafileretrieveerrorreconnectionError`	An error occurred while trying to retrieve the ICA file during reconnection.	Contact your system administrator for assistance.
`NoCWA`	Citrix Workspace app required to open resources.	Install Citrix Workspace app or contact your system administrator for assistance.
`CouldNotFindStore`	Unable to retrieve the required store configuration to launch the resource.	Remove the store from Citrix Workspace app, then add it again. If the issue persists, contact your system administrator.
`noclientinstalled`	Unable to retrieve the required information to launch the resource.	Refresh Citrix Workspace app or log out and back in.
`AuthCancelled`	The authentication session expired.	To try to resolve the issue, reauthenticate in Citrix Workspace app. If the issue persists, contact your system administrator.
`IcaFileLaunchError`	An error occurred while trying to start the ICA file.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`CouldNotContactStore`	An error occurred while trying to communicate with the	Quit and reopen Citrix Workspace app. If the issue

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR ID	DESCRIPTION	RECOMMENDATION
	VDA. This might be due to a server connection issue.	persists, contact your system administrator.
`CCMError`	Unable to launch the resource due to a Connection Manager error. Error code: {errorCodeValue}	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`CCMInitFailed`	Unable to launch the resource because the Connection Manager failed to initialize.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`CCMLoadFailed`	Unable to launch the resource because the Connection Manager failed to load.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`InvalidIcaParams`	Unable to launch the resource due to incorrect ICA parameters.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`AppExiting`	Unable to launch the resource because the Citrix Workspace app is exiting.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`UTF8ConversionFailed`	Unable to parse the ICA file.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`MissingSoftware`	You need additional software to use this app.	Contact your system administrator for assistance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app for Mac

ERROR ID	DESCRIPTION	RECOMMENDATION
`AuthCancelled`	The authentication session expired.	To try to resolve the issue, first authenticate with your credentials. If the issue persists, contact your system administrator.
`NetworkError`	Unable to launch the resource due to a network connection issue.	Check your connection and try again. If the issue persists, contact your system administrator.
`ViewerNotFound`	The Citrix Viewer path cannot be found.	To try to resolve the issue, uninstall and reinstall Citrix Workspace app. If the issue persists, contact your system administrator.
`ViewerOpenEventFailed`	Citrix Viewer failed to create an event.	Try to launch the resource from your store again. If the issue persists, contact your system administrator.
`ViewerLaunchTimeout`	Citrix Viewer launch timed out.	Try to launch the resource from your store again. If the issue persists, contact your system administrator.
`ViewerLaunchFailure`	Citrix Viewer failed to launch.	Try to launch the resource from your store again. If the issue persists, contact your system administrator.
`InvalidICAFile`	Unable to launch the resource because the ICA file is invalid.	Try to launch the resource from your store again. If the issue persists, contact your system administrator.
`CertificateError`	An error occurred with the server certificate.	Contact your system administrator for assistance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR ID	DESCRIPTION	RECOMMENDATION
`ResourceError`	An error occurred while trying to start the resource. This might be due to a server connection issue.	Wait a few minutes, then try again. If the issue persists, contact your system administrator.
`UnknownError`	An unknown error occurred while trying to open the resource.	Wait a few minutes, then try again. If the issue persists, contact your system administrator.

Citrix Workspace app for iOS

ERROR ID	DESCRIPTION	RECOMMENDATION
`credentialsMustChange`	Your password must be changed.	Go to your account settings to change your password. If the issue persists, contact your system administrator.
`noConfigurationFile`	Unable to retrieve the required configuration data.	To try to resolve the issue, remove the store from Citrix Workspace app, then add it again. If the issue persists, contact your system administrator.
`http404Error`	Resources are unavailable.	Contact your system administrator for assistance.
`invalidTransactionId`	Invalid transaction ID.	Wait a few minutes, then try again. If the issue persists, contact your system administrator.
`credentialsExpired`	Your password expired.	Go to your account settings to change your password. If the issue persists, contact your system administrator.
`badAddressError`	Unable to find the resource address.	Check your connection and try again. If the issue persists,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR ID	DESCRIPTION	RECOMMENDATION
		contact your system administrator.
`accountDisabled`	Your account is disabled.	Contact your system administrator for assistance.
`accountLockedOut`	Your account is temporarily locked.	Contact your system administrator for assistance.
`storeServerConnectionError`	An error occurred while trying to communicate with the server.	Wait a few minutes, then try again. If the issue persists, contact your system administrator.
`internalServerError`	An unknown error occurred while trying to connect to the server.	Contact your system administrator for assistance.
`invalidXML`	Unable to open the resource due to an error from the XML service.	Contact your system administrator for assistance.
`badCredentials`	Your credentials expired.	To try to resolve the issue, log out of Citrix Workspace app and then log back in. If the issue persists, contact your system administrator.
`appRemoved`	Resource was removed or disabled by your administrator.	For an up-to-date list of available apps and desktops, either refresh Citrix Workspace app or log out and back in.
`invalidLogonHours`	Unable to log in at this time due to restrictions set by your administrator.	Try again during regular working hours. If the issue persists, contact your system administrator.
`connectionError`	Unable to connect to the server. This can be due to a network connection issue.	To try to resolve the issue, quit and reopen Citrix Workspace app. If the issue

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR ID	DESCRIPTION	RECOMMENDATION
		persists, contact your system administrator.

Citrix Workspace app for Android

ERROR ID	DESCRIPTION	RECOMMENDATION
`http404Error`	Unable to launch the resource due to a network connection issue.	Check your connection and try again. If the issue persists, contact your system administrator.
`couldNotConnectToWorkstation`	Unable to connect to the desktop.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`retryReasonRebooting`	An error occurred while launching resource. The requested workstation is rebooting.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`retryReasonResuming`	An error occurred while launching resource. The requested workstation is resuming.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`generalProblem`	Something went wrong while trying to open the resource.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`retryReasonUnknown`	An error occurred in the ICA file.	Quit and reopen Citrix Workspace app. If the issue persists, contact your system administrator.
`appRemoved`	The resource was removed or disabled by your administrator.	For an up-to-date list of available apps and desktops, either refresh the Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR ID	DESCRIPTION	RECOMMENDATION
		Workspace app or log out and log in.
`resourceError`	An error occurred while trying to start the ICA file.	Wait a few minutes, then try again. If the issue persists, contact your system administrator. Restart VDA if it's a dedicated machine.
`resourceUnavailable`	An error occurred while trying to start the ICA file.	Wait a few minutes, then try again. If the issue persists, contact your system administrator. Restart VDA if it's a dedicated machine.

Troubleshoot VDA registration and session launch issues

We offer a health check feature that lets you gauge the health of VDAs. The feature lets you identify possible causes for common VDA registration and session launch issues using Studio.

Unlike Cloud Health Check, a standalone tool for gauging the health and availability of the site and its other components, the feature is available as the **Run Health Check** action in Studio.

The **Run Health Check** action can run the same checks as Cloud Health Check except the following ones:

- For VDA registration:
  - VDA communication port availability
- For session launches on VDAs:
  - Session launch communication port availability
  - VDA application launch path

Prerequisites

Before you use the feature, verify that you meet the following prerequisites:

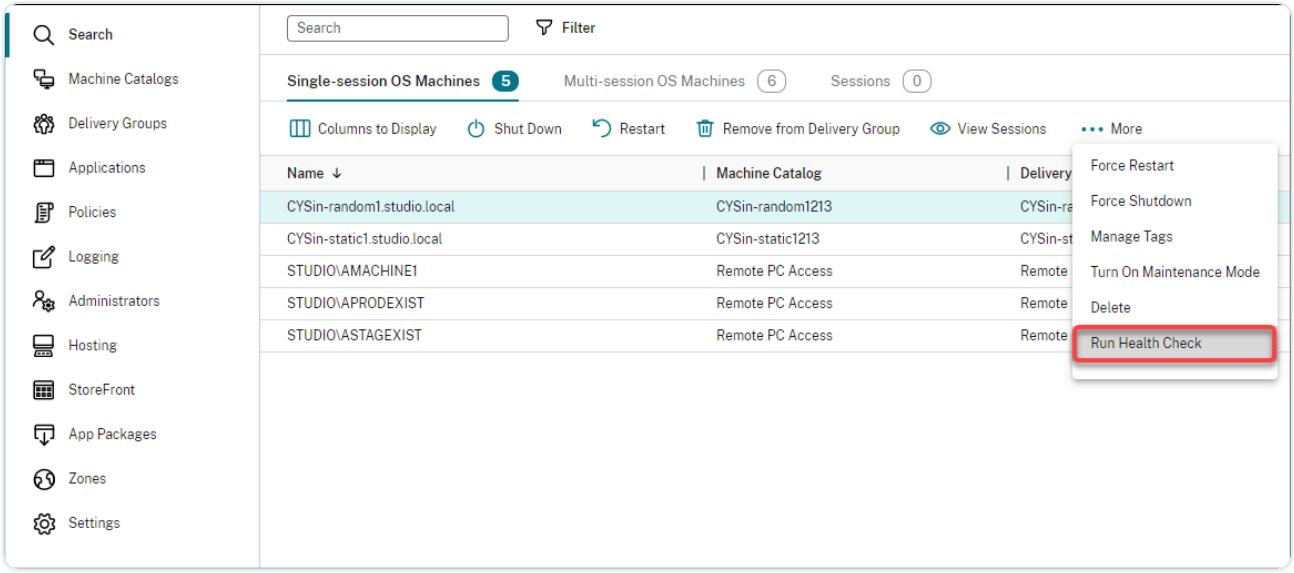
- Windows VDAs
- VDA version 2109 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VDAs are registered

Run health checks for VDAs

1. In Studio, go to the **Search** node.
2. Select one or more machines and then select **Run Health Check** from the action bar.



NOTE:

Currently, you can run health checks only for registered VDAs. The **Run Health Check** action is unavailable for unregistered VDAs.

After you select **Run Health Check**, a window appears, displaying the progress of the health checks. Wait until the heath checks complete or click **Cancel** to cancel the checks. If necessary, you can move the window.



NOTE:

In scenarios where a "health checks in progress" window already exists, you cannot run additional health checks until the existing health checks complete.

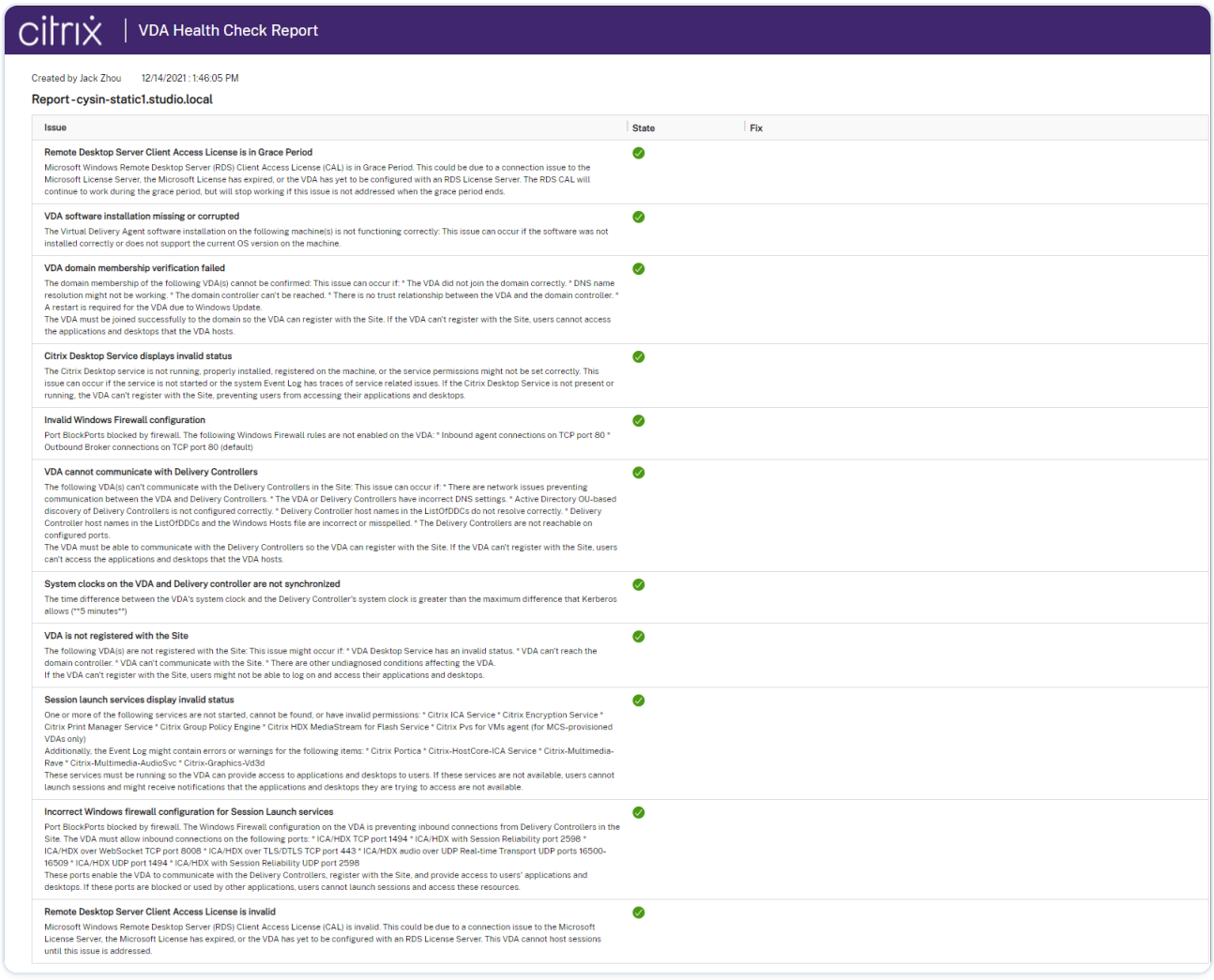
After the health checks complete, the following two buttons appear: **View report** and **Close**. To view the results of the health checks, click **View report**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The health check report opens in a new browser tab. The report contains the following elements:

- Time and date when the results report was generated
- The person who ran the health checks
- Checks run on the target machines
- Issues found, along with fix recommendations



You can run health checks individually and in batches.

NOTE:

When running health checks in batches, select no more than 10 machines. Otherwise, the **Run Health Check** action is unavailable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User access

There are two primary components that provide access to applications and desktops in Citrix DaaS™ deployments:

- **Citrix® StoreFront Cloud**: Citrix® StoreFront Cloud is a service managed by Citrix. This is the simplest way to provide access to DaaS resources, requiring no deployment effort and always kept up to date with the latest features.
- **Citrix StoreFront**: Citrix StoreFront is an on-premises product that you install in your own environment. This is recommended when you need to aggregate resources from DaaS and on-prem CVAD deployments or where you need more control of the deployment. You can deploy a Citrix Gateway to allow users to authenticate and connect to StoreFront from outside your internal network.

In either case, end-users access their workspaces or stores using Citrix Workspace app, either in a web browser or a locally installed app.

Using Citrix® StoreFront Cloud

Access to stores occurs through one or more URLs `https://<subdomain>.cloud.com`, where you can choose `<subdomain>`. Alternatively you can register your own custom domain.

For more information about using Citrix® StoreFront Cloud, see:

- Configure access: For configuring access.
- Configure authentication: For configuring authentication.
- Manage your workspace experience: For understanding how end-users access their workspace and how it appears.

To provide remote access to the resources managed by DaaS, you can use either Citrix Gateway service or your own Citrix Gateway. For more information on configuring remote access to resources, see Connectivity to DaaS resources.

Service continuity

Service continuity allows users to connect resources when Citrix Cloud is not available. For more information, see Service continuity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using on-premises StoreFront

StoreFront is a Windows application that you can install on your own servers to provide access to CVAD, DaaS and SPA resources. It connects to DaaS using Citrix Cloud Connectors that proxies the requests to Citrix Cloud. The connector encrypts passwords before they are sent to Citrix Cloud, using a key that is returned directly to Citrix Workspace app and never sent to the cloud.

1. Install the connectors and enable HTTPS. You should have at least two connectors in each location for redundancy.
2. Ensure the Cloud Connector can reach the Cloud NFuse/STA URL at (`https://<customername\>.xendesktop.net/Scripts/wpnbr.dll` and `ctxsta.dll`).
3. If you do not already have a StoreFront deployment, Install StoreFront and Create a deployment.
4. Add a site to your store. In the server list include all cloud connectors from all resource locations. Choose the HTTPS protocol.

End user access

To provide access to end-users using Citrix Workspace app, see User access options

Remote access using Citrix Gateway

You should not expose your StoreFront server directly to the internet. Instead provide authentication and remote access using Citrix Gateway. You can also use a Citrix Gateway for internal access to take advantage of its security features.

- Deploy a NetScaler Gateway appliance. See the NetScaler Gateway documentation for details.
- Configure the Gateway for remote access to your store. For the STA servers, you can use the Cloud Connectors.
- Add the Citrix Gateway to StoreFront. Use the same list of STA servers you configured on your gateway.

Local Host Cache

Local Host Cache enables connection brokering operations in Citrix DaaS deployment to continue when Cloud Connectors cannot communicate with Citrix Cloud.

The Local Host Cache feature requires a customer-deployed on-premises Citrix® StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Each resource location must have a customer-deployed on-premises StoreFront. Verify that the resource location contains a local StoreFront that points to all the Cloud Connectors in that resource location.

For more information, see Local Host Cache.

Virtual IP and virtual loopback

IMPORTANT:

Windows 10 Enterprise multi-session doesn’t support Remote Desktop IP Virtualization (Virtual IP) and we don't support Virtual IP nor virtual loopback on Windows 10 Enterprise multi-session.

Virtual IP and virtual loopback features are supported on Windows Server 2016 machines. These features do not apply to Windows desktop OS machines.

The Microsoft virtual IP address feature provides a published application with a unique dynamically assigned IP address for each session. The Citrix virtual loopback feature allows you to configure applications that depend on communications with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.*).

Certain applications, such as CRM and Computer Telephony Integration (CTI), use an IP address for addressing, licensing, identification, or other purposes and thus require a unique IP address or a loopback address in sessions. Other applications may bind to a static port, so attempts to launch additional instances of an application in a multiuser environment will fail because the port is already in use. For such applications to function correctly in a Citrix Virtual Apps™ environment, a unique IP address is required for each device.

Virtual IP and virtual loopback are independent features. You can use either or both.

Administrator action synopsis:

- To use Microsoft virtual IP, enable and configure it on the Windows server. (Citrix® policy settings are not needed.)
- To use Citrix virtual loopback, configure two settings in a Citrix policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual IP

When virtual IP is enabled and configured on the Windows server, each configured application running in a session appears to have a unique address. Users access these applications on a Citrix Virtual Apps server in the same way they access any other published application. A process requires virtual IP in either of the following cases:

- The process uses a hard-coded TCP port number
- The process uses Windows sockets and requires a unique IP address or a specified TCP port number

To determine if an application needs to use virtual IP addresses:

1. Obtain the TCPView tool from Microsoft. This tool lists all applications that bind specific IP addresses and ports.
2. Disable the Resolve IP Addresses feature so that you see the addresses instead of host names.
3. Launch the application and use TCPView to see which IP addresses and ports are opened by the application and which process names are opening these ports.
4. Configure any processes that open the IP address of the server, 0.0.0.0, or 127.0.0.1.
5. To ensure that an application does not open the same IP address on a different port, launch an additional instance of the application.

How Microsoft Remote Desktop (RD) IP virtualization works

- Virtual IP addressing must be enabled on the Microsoft server.

  For example, in a Windows Server 2016 environment, from Server Manager, expand **Remote Desktop Services > RD Session Host Connections** to enable the RD IP Virtualization feature and configure the settings to dynamically assign IP addresses using the Dynamic Host Configuration Protocol (DHCP) server on a per-session or per-program basis. See the Microsoft documentation for instructions.
- After the feature is enabled, at session start-up, the server requests dynamically assigned IP addresses from the DHCP server.
- The RD IP Virtualization feature assigns IP addresses to remote desktop connections per-session or per-program. If you assign IP addresses for multiple programs, they share a per-session IP address.
- After an address is assigned to a session, the session uses the virtual address rather than the primary IP address for the system whenever the following calls are made:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

When using the Microsoft IP virtualization feature within the Remote Desktop session hosting configuration, applications are bound to specific IP addresses by inserting a “filter” component between the application and Winsock function calls. The application then sees only the IP address it should use. Any attempt by the application to listen for TCP or UDP communications is bound to its allocated virtual IP address (or loopback address) automatically, and any originating connections opened by the application originate from the IP address bound to the application.

In functions that return an address (such as `GetAddrInfo()`, which is controlled by a Windows policy), if the local host IP address is requested, virtual IP looks at the returned IP address and changes it to the virtual IP address of the session. Applications that attempt to get the IP address of the local server through such name functions see only the unique virtual IP address assigned to that session. This IP address is often used in subsequent socket calls, such as bind or connect. For more information about Windows policies, see RDS IP Virtualization in Windows Server.

Often, an application requests to bind to a port for listening on the address 0.0.0.0. When an application does this and uses a static port, you cannot launch more than one instance of the application. The virtual IP address feature also looks for 0.0.0.0 in these call types and changes the call to listen on the specific virtual IP address, which enables more than one application to listen on the same port on the same computer because they are all listening on different addresses. The call is changed only if it is in an ICA session and the virtual IP address feature is enabled. For example, if two instances of an application running in different sessions both try to bind to all interfaces (0.0.0.0) and a specific port (such as 9000), they are bound to VIPAddress1:9000 and VIPAddress2:9000 and there is no conflict.

Virtual loopback

Enabling the Citrix virtual IP loopback policy settings allows each session to have its own loopback address for communication. When an application uses the localhost address (default = 127.0.0.1) in a Winsock call, the virtual loopback feature simply replaces 127.0.0.1 with 127.X.X.X, where X.X.X is a representation of the session ID + 1. For example, a session ID of 7 is 127.0.0.8. In the unlikely event that the session ID exceeds the fourth octet (more than 255), the address rolls over to the next octet (127.0.1.0), to the maximum of 127.255.255.255.

A process requires virtual loopback in either of the following cases:

- The process uses the Windows socket loopback (localhost) address (127.0.0.1)
- The process uses a hard-coded TCP port number

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use the virtual loopback policy settings for applications that use a loopback address for interprocess communication. No additional configuration is required. Virtual loopback has no dependency on Virtual IP, so you do not have to configure the Microsoft server.

- Virtual IP loopback support. When enabled, this policy setting allows each session to have its own virtual loopback address. This setting is disabled by default. The feature applies only to applications specified with the Virtual IP virtual loopback programs list policy setting.
- Virtual IP virtual loopback programs list. This policy setting specifies the applications that use the virtual IP loopback feature. This setting applies only when the Virtual IP loopback support policy setting is enabled.

Related feature

You can use the following registry settings to ensure that virtual loopback is given preference over virtual IP; this is called preferred loopback. However, proceed with caution:

- Use preferred loopback only if both Virtual IP and virtual loopback are enabled; otherwise, you may have unintended results.
- Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Run regedit on the servers where the applications reside.

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- Name: PreferLoopback, Type: REG_DWORD, Data: 1
- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: \<list of processes\>

Zones

Introduction

Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) deployments that span widely dispersed locations connected by a WAN can face challenges from network latency and reliability. Using zones can help users in remote regions connect to resources without necessarily forcing their connections to traverse large segments of the WAN. In Citrix DaaS environment, each resource location is considered a zone.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zones can be helpful in deployments of all sizes. You can use zones to keep applications and desktops closer to users, which improves performance. Zones can be used for disaster recovery, geographically distant data centers, branch offices, a cloud, or an availability zone in a cloud.

Throughout this article, the term local refers to the zone being discussed. For example, "A VDA registers with a local Cloud Connector" means that a VDA registers with a Cloud Connector in the zone where the VDA is located.

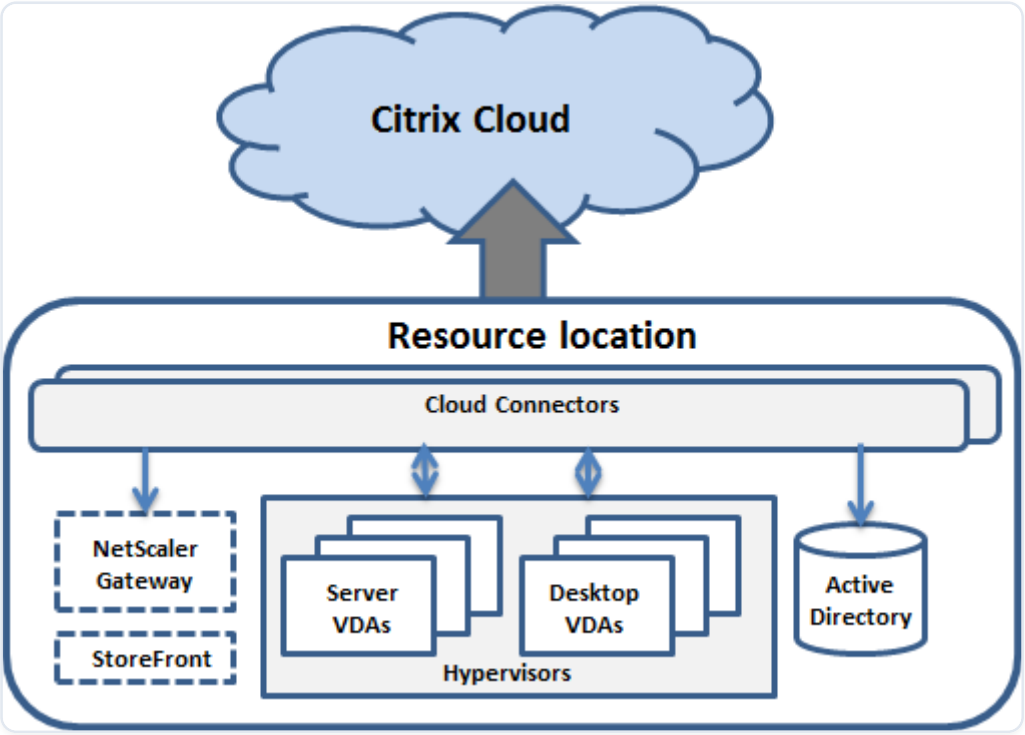
Differences from zones in on-premises Citrix Virtual Apps and Desktops environments

Zones in Citrix DaaS™ environment are similar, but not identical to zones in an on-premises Citrix Virtual Apps and Desktops deployment.

- In Citrix DaaS, zones are created automatically when you create a resource location and add a Cloud Connector to it. Unlike an on-premises deployment, Citrix DaaS environment does not classify zones as primary or satellite.
- In XenApp version 6.5 and earlier, zones included data collectors. Citrix DaaS does not use data collectors for zones. Also, failover and preferred zones work differently.

What's in a zone

A zone is equivalent to a resource location. When you create a resource location and install a Cloud Connector, a zone is automatically created for you. Each zone can have a different set of resources, based on your unique needs and environment.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Each zone must always have at least one Cloud Connector, and preferably two or more, for redundancy.

You can place machine catalogs, hypervisors, host connections, users, and applications in a zone. A zone can also contain a Citrix Gateway.

Placing items in a zone affects how Citrix DaaS interacts with them and with other objects related to them.

- When a hypervisor connection is placed in a zone, it is assumed that all the hypervisors managed through that connection also reside in that zone.
- When a machine catalog is placed in a zone, it is assumed that all VDAs in the catalog are in the zone.
- Citrix Gateway instances can be added to zones. When you create a resource location, you are offered the option to add a Citrix Gateway. When a Citrix Gateway is associated with a zone, it is preferred for use when connections to VDAs in that zone are used.
- Ideally, Citrix Gateway in a zone is used for user connections coming into that zone from other zones or external locations. You can also use it for connections within the zone.
- After you create more resource locations and install Cloud Connectors in them (which automatically creates more zones), you can move resources between zones. This flexibility comes with the risk of separating items that work best in close proximity. For example, moving a catalog to a different zone than the connection (host) that creates the machines in the catalog, can affect performance. So, consider potential unintended effects before moving items between zones. Keep a catalog and the host connection it uses in the same zone.

If the connection between a zone and Citrix Cloud fails, the Local Host Cache feature enables a Cloud Connector in the zone to continue brokering connections to VDAs in that zone. (The zone must have StoreFront installed.) For example, this is effective in an office where workers use the local StoreFront site to access their local resources, even if the WAN link connecting their office to the corporate network fails. For more information, see Local Host Cache.

Where VDAs register

VDAs must be minimum version 7.7 to use these zone registration features:

- A VDA in a zone registers with a local Cloud Connector.
    - As long as that Cloud Connector can communicate with Citrix Cloud™, normal operations continue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - If that Cloud Connector is operational but cannot communicate with Citrix Cloud (and that zone has a local StoreFront), it enters Local Host Cache outage mode.
    - If a Cloud Connector fails, VDAs in that zone attempt to register with other local Cloud Connectors. A VDA in one zone never attempts to register with a Cloud Connector in another zone.

- If you add or remove a Cloud Connector in a zone (using the Citrix Cloud management console), and auto-update is enabled, VDAs in that zone receive updated lists of available local Cloud Connectors, so they know with whom they can register and accept connections from.
- If you move a machine catalog to another zone (using Studio), the VDAs in that catalog re-register with Cloud Connectors in the zone where you moved the catalog. When you move a catalog, ensure you also move any associated host connection to the same zone.
- During an outage (when Cloud Connectors in a zone cannot communicate with Citrix Cloud), only the resources associated with machines that are registered in that zone are available.

Zone preference

In a multi-zone Site, the zone preference feature offers the administrator more flexibility to control which VDA is used to launch an application or desktop.

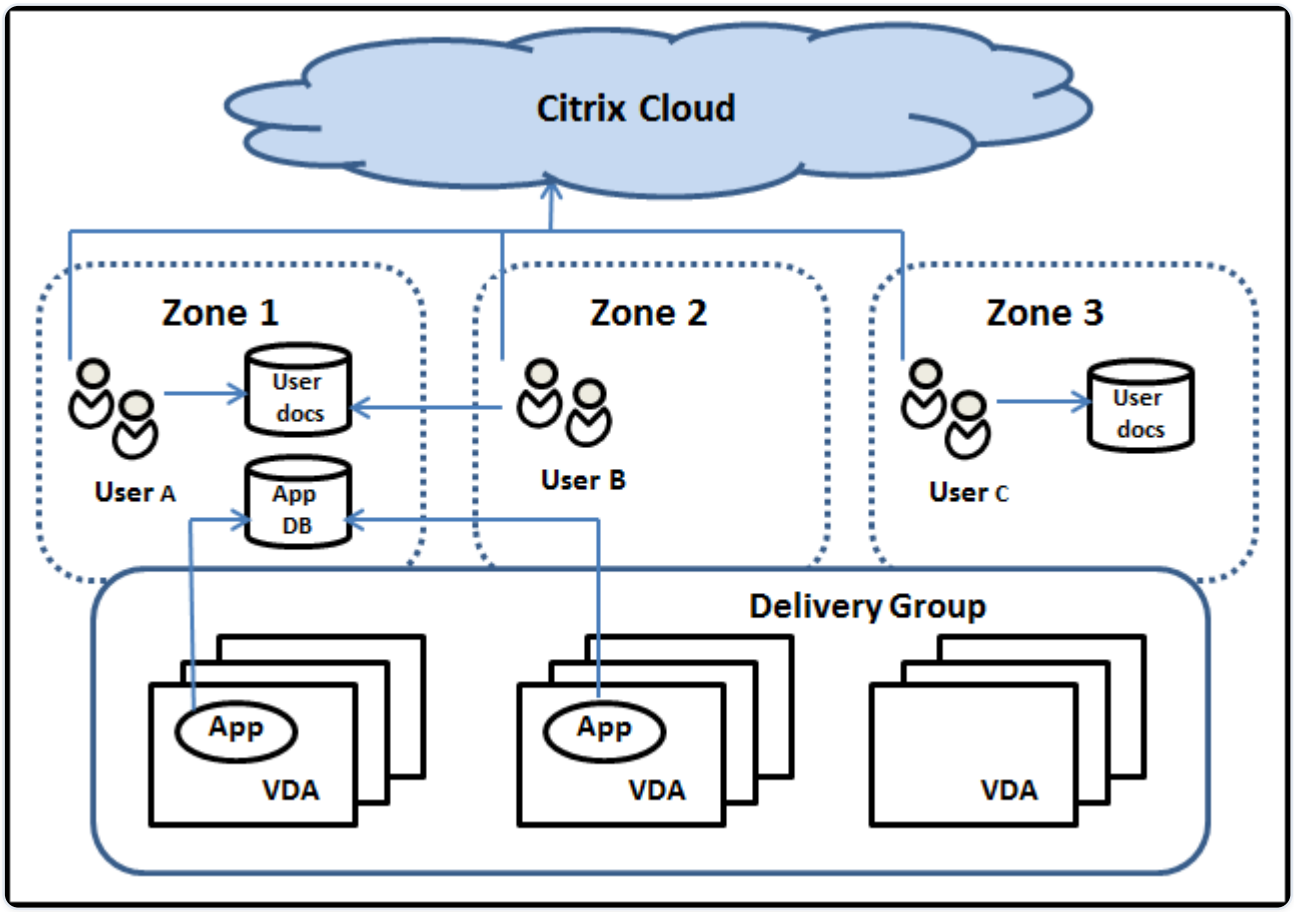
How zone preference works

There are three forms of zone preference. You might prefer to use a VDA in a particular zone, based on:

- Where the application's data is stored. This is referred to as the application home.
- The location of the user's home data, such as a profile or home share. This is referred to as the user home.
- The user's current location (where the Citrix Workspace app is running). This is referred to as the user location. User location requires minimum StoreFront 3.7 and Citrix Gateway (formerly NetScaler Gateway) 11.0-65.x.

The following graphic shows an example multi-zone configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this example, VDAs are spread among three zones, but they are all in the same delivery group. Therefore, Citrix DaaS broker might have a choice which VDA to use for a user launch request. This example illustrates that users can be running their Citrix Workspace app endpoints at different locations. User A is using a device with Citrix Workspace app in zone 1. User B is using a device in zone 2. Similarly, a user's documents can be stored in different locations. Users A and B use a share located in zone 1. User C uses a share in zone 3. Also, one of the published applications uses a database located in zone 1.

You associate a user or application with a zone by configuring a home zone for the user or application. The broker then uses those associations to help select the zone where a session will be launched, if resources are available. You:

- Configure the home zone for a user by adding a user to a zone.
- Configure the home zone for an application by editing the application's properties.

A user or an application can have only one home zone at a time. (An exception for users can occur when multiple zone memberships occur because of user group membership. However, even in this case, the broker uses only one home zone.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Although zone preferences for users and applications can be configured, the broker selects only one preferred zone for a launch. The default priority order for selecting the preferred zone is: application home > user home > user location. When a user launches an application:

- If that application has a configured zone association (an application home), then the preferred zone is the home zone for that application.
- If the application does not have a configured zone association, but the user does (a user home), then the preferred zone is the home zone for that user.
- If neither the application nor the user has a configured zone association, then the preferred zone is the zone where the user is running a Citrix Workspace app instance (the user location). If that zone is not defined, a random VDA and zone selection is used. Load balancing is applied to all VDAs in the preferred zone. If there is no preferred zone, load balancing is applied to all VDAs in the delivery group.

Tailoring zone preference

When you configure (or remove) a home zone for a user or an application, you can also further restrict how zone preference is (or is not) used.

- **Mandatory user home zone use:** In a delivery group, you can specify "Launch the session in the user's home zone (if the user has a home zone), with no failover to a different zone if resources are not available in the home zone." This restriction is helpful if you want to avoid the risk of copying large profiles or data files between zones. In other words, you would rather deny a session launch than launch the session in a different zone.
- **Mandatory application home zone use:** Similarly, when you configure a home zone for an application, you can specify "launch the application only in that zone, with no failover to a different zone if resources are not available in the application's home zone."
- **No application home zone, and ignore configured user home zone:** If you do not specify a home zone for an application, you can also specify "do not consider any configured user zones when launching that application." For example, use the user location zone preference if you want users to run a specific application on a VDA close to their machine, even though some users might have a different home zone.

How preferred zones affect session use

When a user launches an application or desktop, the broker prefers using the preferred zone rather than using an existing session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the user launching an application or desktop already has a session that is suitable for the resource being launched (for example, can use session sharing for an application, or a session already running the resource being launched), but that session is on a VDA in a zone other than the preferred zone for the user/application, then the system might create a new session. This action satisfies launching in the correct zone (if it has available capacity), ahead of reconnecting to a session in a less-preferred zone for that user's session requirements.

To prevent an orphan session that can no longer be reached, reconnection is allowed to existing disconnected sessions, even if they are in a non-preferred zone.

The order of desirability for sessions to satisfy a launch is:

1. Reconnect to an existing session in the preferred zone.
2. Reconnect to an existing disconnected session in a non-preferred zone.
3. Start a new session in the preferred zone.
4. Reconnect to a connected existing session in a non-preferred zone.
5. Start a new session in a non-preferred zone.

Other zone preference considerations

- If you configure a home zone for a user group (such as a security group), that group's users (through direct or indirect membership) are associated with the specified zone. However, a user can be a member of multiple security groups, and therefore might have a different home zone configured through other group membership. In such cases, determination of that user's home zone can be ambiguous.

  If a user has a configured home zone that was not acquired through group membership, that zone is used for zone preference. Any zone associations acquired through group membership are ignored.

  If the user has multiple different zone associations acquired solely through group membership, the broker chooses among the zones randomly. After the broker makes this choice, that zone is used for subsequent session launches, until the user's group membership changes.
- The user location zone preference requires detection of Citrix Workspace app on the endpoint device by the Citrix Gateway through which that device is connecting. The Citrix must be configured to associate ranges of IP addresses with particular zones. Discovered zone identity must be passed through StoreFront to Citrix DaaS.

Although written for on-premises use of zones, the Zone Preference Internals blog post contains relevant technical details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Permissions to manage zones

A Full Administrator can perform all supported zone management tasks. Moving items between zones does not require zone-related permissions (except zone read permission). However, you must have edit permission for the items you are moving. For example, to move a machine catalog from one zone to another, you must have edit permission for that catalog.

If you use Citrix Provisioning™: The current Citrix Provisioning console is not aware of zones, so Citrix recommends using Studio to create machine catalogs that you want to place in specific zones. After you create the catalog, you can use the Citrix Provisioning console to provision machines in that catalog.

Zone creation

When you create a resource location in Citrix Cloud and then add a Cloud Connector to that resource location, Citrix DaaS automatically creates and names a zone. You can optionally add a description later.

After you create more than one resource location (and the zones are created automatically), you can move resources from one zone to another.

Resource locations and zones are synchronized periodically, typically and approximately every five minutes. So, if you change a resource location's name in Citrix Cloud, that change is propagated to the associated zone within five minutes.

Add or change a zone description

Although you cannot change a zone's name, you can add or change its description.

1. From Studio, select **Zones** in the left pane.
2. Select a zone in the middle pane and then select **Edit Zone** in the action bar.
3. Add or change the zone description.
4. Select **Save** or **Apply.**

Assign scopes to a zone

Assign scopes to a zone to grant custom administrators scoped access to specific zones. Scope control helps you align administrative access with your organization's operational and security requirements.

To assign scopes to a zone, you must have the **Edit zone scope** permission.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. From Studio, select **Zones** in the left pane.
2. Select a zone in the middle pane, and then select **Edit Zone** in the action bar.
3. Select the scopes you want to assign to the zone.
4. If the **Bypass scope control for this resource** checkbox is selected, the zone is visible to all administrators. To apply scope control, clear the checkbox, and then select the scopes you want.
5. Select **Save** or **Apply.**

Move resources from one zone to another zone

1. From Studio, select **Zones** in the left pane.
2. Select a zone in the middle pane, and then select one or more items.
3. Either drag the items to the destination zone or select **Move Items** in the action bar, and then specify which zone to move them to. (Although you can select Cloud Connectors, you cannot actually move them to a different zone.)

A confirmation message lists the items you selected and asks if you are sure that you want to move all of them.

Remember: When a machine catalog uses a host connection to a hypervisor or cloud service, ensure that the catalog and the connection are in the same zone. Otherwise, performance can be affected. If you move one, move the other, too.

Zone deletion

You cannot delete a zone. However, you can delete a resource location (after removing its Cloud Connectors). Deleting the resource location automatically deletes the zone.

- If the zone does not contain any items (such as catalogs, connections, applications, or users), the zone is deleted during the next synchronization between zones and resource locations. Synchronization occurs every five minutes.
- If the zone contains items, the zone is automatically deleted after all items are removed.

Add a home zone for a user

Configuring a home zone for a user is also known as *adding a user to a zone*.

1. From Studio, select **Zones** in the left pane.
2. Select a zone in the middle pane and then select **Add Users to Zone** in the action bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **Add Users to Zone** dialog box, select **Add**, and then select the users and user groups to add to the zone. If you specify users who already have a home zone, a message offers two choices: **Yes** = add only those users you specified who do not have a home zone; **No** = return to the user selection dialog.
4. Select **OK**.

For users with a configured home zone, you can require that sessions launch only from their home zone:

1. Create or edit a delivery group.
2. On the **Users** page, select the **Require sessions to launch in a user's home zone (if configured)** check box.

All sessions launched by a user in that delivery group must launch from machines in that user's home zone. If a user in the delivery group does not have a configured home zone, this setting has no effect.

Remove a home zone for a user

This procedure is also known as removing a user from a zone.

1. From Studio, select **Zones** in the left pane.
2. Select a zone in the middle pane and then select **Remove Users from Zone** in the action bar.
3. In the **Add Users to Zone** dialog box, select **Remove**, and then select the users and groups to remove from the zone. This action removes the users only from the zone. Those users remain in the delivery groups to which they belong.
4. Confirm the removal when prompted.

Manage home zones for applications

Configuring a home zone for an application is also known as adding an application to a zone. By default, in a multi-zone environment, an application does not have a home zone.

An application's home zone is specified in the application's properties. You can configure application properties when you add the application to a group or later.

- When creating a delivery group or adding applications to existing groups, select **Properties** on the **Applications** page of the wizard.
- To change an application's properties after the application is added, select **Zones** in the left pane. Select an application and then select **Properties** in the action bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On the **Zones** page of the application's properties/settings:

- If you want the application to have a home zone:
  - Select the **Use the selected zone to decide** radio button and then select the zone.
  - If you want the application to launch only from the selected zone (and not from any other zone), select the check box under the zone selection.
- If you do not want the application to have a home zone:
  - Select the **Do not configure a home zone** radio button.
  - If you do not want the broker to consider any configured user zones when launching this application, select the check box under the radio button. In this case, neither application nor user home zones are used to determine where to launch this application.

Other actions that include specifying zones

If you have more than one zone, you can specify a zone when you add a host connection or create a catalog. Zones are listed alphabetically in selection lists. By default, the first alphabetical name is selected.

Troubleshooting

Studio gives you proactive alerts to make sure that your Local Host Cache and zones are configured correctly so that you can resolve the issues in time before an outage impacts your users. This feature helps in maintaining continued user access to mission-critical workloads.

A **Troubleshoot** tab appears for each zone with issues.

To check zone-related issues, follow these steps:

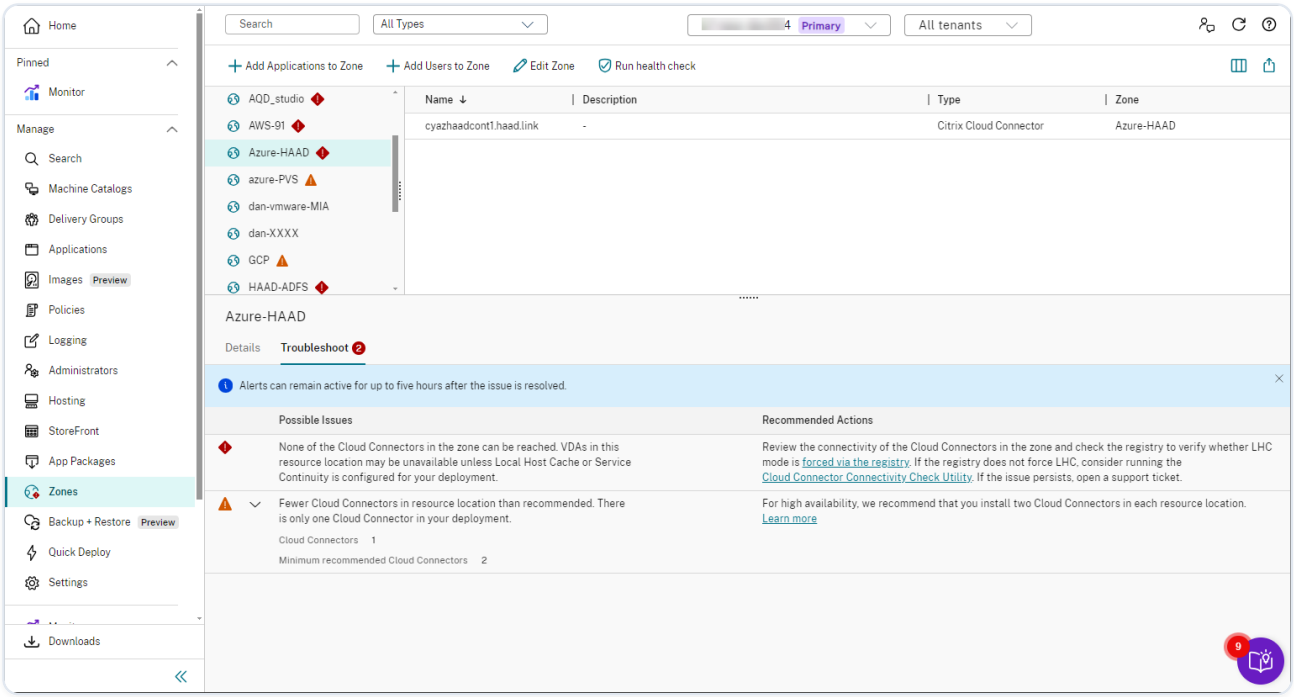
1. Go to **Zones** and click the zone with the warning icon.
2. Go to the **Troubleshoot** tab in the lower pane and read the information there.

NOTE:

Diagnostics are updated on an hourly basis.

Troubleshooting information example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following table provides a complete list of zone-related warnings and errors:

SEVERITY	POSSIBLE ISSUES	RECOMMENDED ACTIONS
Warning	Resource location contains multiple domains. Resource locations that contain multiple domains may cause delayed or failed VDA registrations when in Local Host Cache mode.	Reconfigure your resource location so all Cloud Connectors are in the same domain. Refer to the Citrix Cloud Connector Technical Details for more information about supported multi-domain configurations.
Warning	The number of host connections in the resource location exceeds the recommended limit, which might result in performance degradation.	Reduce the number of host connections in the resource location to no more than the recommended limit. Refer to Limits.
Warning	There is only one Cloud Connector in the resource location.	For high availability, install two Cloud Connectors in each resource location. Refer to the Citrix Cloud Connector Technical Details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SEVERITY	POSSIBLE ISSUES	RECOMMENDED ACTIONS
Warning	There are fewer CPUs per socket than recommended, which might result in performance degradation in Local Host Cache mode.	Ensure each Cloud Connector meets the minimum CPU per socket requirements. Refer to Recommended compute configuration for Local Host Cache.
Warning	StoreFront is not sending STA requests to all Cloud Connectors in this resource location.	Ensure all Cloud Connectors are added as STA servers on both StoreFront and NetScaler® Gateway to avoid launch failures in Local Host Cache mode.
Warning	StoreFront is detected in the Resource Location, but at least one Connector within the Resource Location is not receiving StoreFront traffic. Missing traffic from StoreFront can affect scalability and cause issues entering high availability mode.	Ensure all Cloud Connectors are listed as a resource feed in StoreFront and check that StoreFront can communicate with all listed Connectors at the port specified in the resource feed.
Warning	Resource location has multiple elected Local Host Cache brokers. Having multiple elected Local Host Cache brokers can cause VDA registrations to be divided among the connectors in Local Host Cache mode, leading to intermittent launch failures.	Ensure connectors can communicate at `http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection`. Refer to Zones with multiple Cloud Connectors.
Warning	There are fewer logical CPU processors than recommended, which might result in performance	Ensure that each Cloud Connector meets the minimum logical CPU processor requirements for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SEVERITY	POSSIBLE ISSUES	RECOMMENDED ACTIONS
	degradation in Local Host Cache mode.	Local Host Cache. Refer to Recommended compute configuration for Local Host Cache.
Warning	There is less RAM than recommended, which might result in performance degradation in Local Host Cache mode.	Ensure that each Cloud Connector meets the minimum RAM requirements for Local Host Cache. Refer to Recommended compute configuration for Local Host Cache.
Error	There are more VDAs in the resource location than recommended, which will result in failed VDA registrations in Local Host Cache mode.	Reduce the number of VDAs in this resource location to no more than the recommended limit. Refer to Limits.
Error	None of the Cloud Connectors in the zone can be reached. VDAs in this resource location should be available through Local Host Cache or Service Continuity.	Review the connectivity of the Cloud Connectors in the zone and check the registry to check if LHC mode is forced via the registry. If LHC is not forced through the registry, consider running the Cloud Connector Connectivity Check Utility. If the issue persists, open a support ticket.
Error	There are fewer logical CPU processors than recommended, which might result in performance degradation.	Ensure that each Cloud Connector meets the minimum logical CPU processor requirements. Refer to Citrix Cloud Connector Technical Details.
Error	There is less RAM than recommended, which might	Ensure that each Cloud Connector meets the minimum RAM requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SEVERITY	POSSIBLE ISSUES	RECOMMENDED ACTIONS
	result in performance degradation.	Refer to Citrix Cloud Connector Technical Details.

To get a detailed misconfigurations report in the zone, run the PowerShell cmdlet, `Get-ConfigMisconfigurationReport`. Added details include information such as which Connector is misconfigured, what is the current misconfiguration, and what is the recommended configuration.

Remove broker user from the cache

There are cases when administrators are unable to remove a broker user from the cache or sometimes when running `Get-BrokerUser`, the user displays the incorrect SID from AD.

This happens when the user is deleted from AD and recreated but the broker cache still has the previous user SID.

To resolve this, do the following:

1. Remove the users from Active Directory.
2. Run `Get-BrokerUser` for each removed account. Accounts that are not referenced anywhere, do not return any results. For users that are referenced, you get a value after you run `Get-BrokerUser`. Now, you must find out what resources the user is assigned to and manually remove the users from those resources.

   For example:

   - Find if the user is assigned to an application: `Get-BrokerApplication`
   - Find if the user is assigned to an application group: `Get-BrokerApplicationGroup`
   - Find if the user is assigned to an access policy: `Get-BrokerAccessPolicyRule`
   - Find if the user is assigned to an application entitlement policy: `Get-BrokerAppEntitlementPolicyRule`
   - Find if the user is assigned to a desktop entitlement policy: `Get-BrokerEntitlementPolicyRule`
   - Find if the user is assigned to a desktop group session linger: `Get-BrokerSessionLinger`
   - Find if the user is running any sessions on a VDA: `Get-BrokerSession`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Find if the user is assigned to a resource in the merged group: `Get-BrokerMergedResource`
- Find if the user is assigned to a group of resources: `Get-BrokerMergeGroup`
- Find if a command is queued for a user: `Get-BrokerMachineCommand`
- Find if the user is assigned to a private desktop: `Get-BrokerMachineV2`
- Find if the user is assigned to a zone preference: `Get-BrokerUserZonePreference`

3. Manually remove the users from the resources.
4. Run `Get-BrokerUser` command to confirm the user has been removed from all resources.
5. Once the user has been removed from all resources, run the following to remove the user from the cache.

```
Update-BrokerNameCache -Users -Purge -UnusedFor 0
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitor

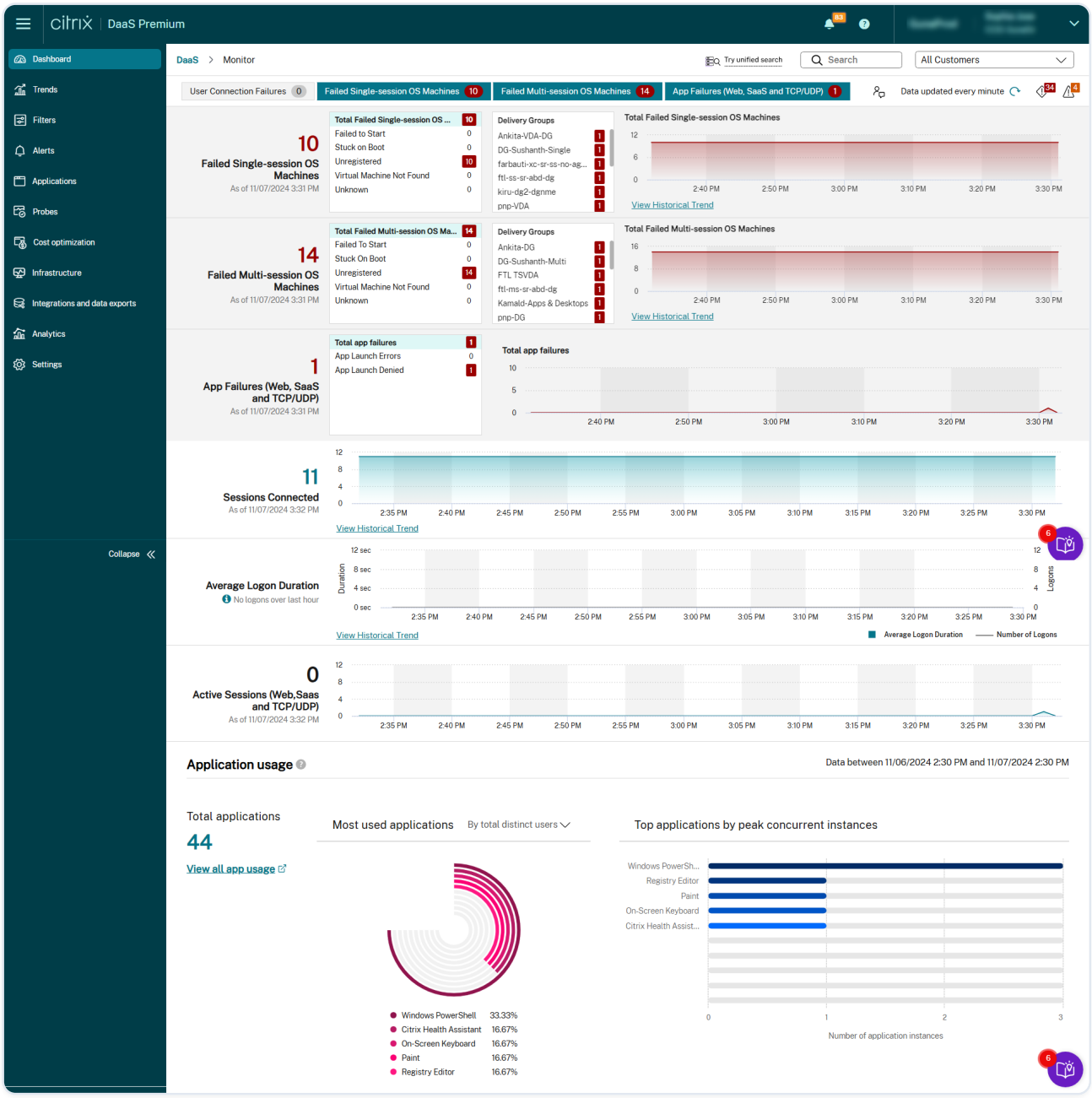
Administrators and help-desk personnel can monitor Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) from **Monitor**, the monitoring and troubleshooting console. The **Monitor** node directs you to a dashboard to monitor, troubleshoot, and perform support tasks for subscribers.

NOTE:

Monitor is available as the Director console to monitor and troubleshoot Citrix Virtual Apps and Desktops Current Release and LTSR deployments.

To access **Monitor**, sign in to Citrix Cloud. In the upper left menu, select **Solutions > DaaS**. Click **Monitor**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

The recommended optimal screen resolution for viewing Citrix Monitor is 1440 x 1024.

Monitor provides:

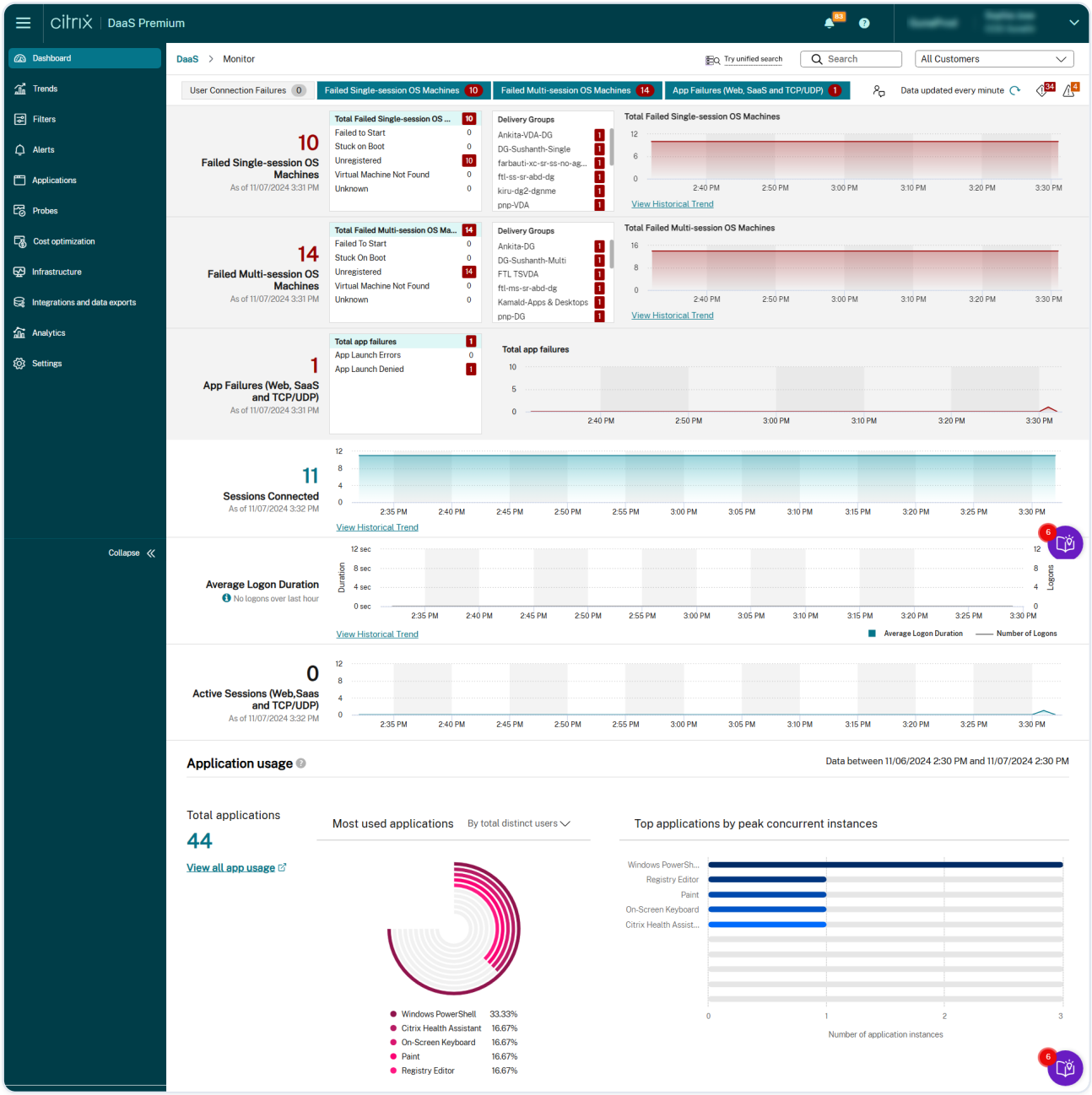
- Real-time data from the Broker Agent using a unified console integrated with Analytics and Performance Manager.
- Analytics includes performance management for health and capacity assurance, and historical trending to identify bottlenecks in your Citrix DaaS™ environment.
- Historical data stored in the Monitor database to access the Configuration Logging database.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Gain visibility into the end-user experience for virtual applications, desktops, and users for Citrix DaaS.
- Monitor uses a troubleshooting dashboard that provides real-time and historical health monitoring of Citrix DaaS. This feature allows you to see failures in real time, providing a better idea of what the end users are experiencing.

Site analytics

The Monitor dashboard provides a centralized location to monitor the health and usage of a site.



If there're currently no failures and no failures have occurred in the past 60 minutes, the panels stay collapsed. When there are failures, the specific failure panel automatically appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PANEL	DESCRIPTION
User Connection Failures	Connection failures over the last 60 minutes. Click the categories next to the total number to view metrics for that type of failure. In the adjacent table, that number is further categorized based on each delivery group. Connection failures include failures caused by application limits being reached. For more information on application limits, see Applications.
Failed Single-session OS Machines or Failed Multi-session OS Machines	Total failures in the last 60 minutes categorized based on each delivery groups. Failures broken out by types, including failed to start, stuck on boot, and unregistered. For Multi-session OS machines, failures also include machines reaching maximum load.
Sessions Connected	Connected sessions across all delivery groups for the last 60 minutes.
Average Logon Duration	Log on data for the last 60 minutes. The large number on the left is the average logon duration across the hour. Log on data for VDAs earlier than XenDesktop 7.0 isn't included in this average. For more information, see Diagnose user logon issues.
Total connected users	Shows the number of users who had at least one connection in the last 24 hours or last 7 days. This panel helps the admins to showcase adoption trends to their executives.
Citrix Workspace™ app versions found in your environment	Provides an overview of the Citrix Workspace app versions used across the organization. It helps in unifying the versions by showing how many devices are using different versions. By default, Citrix Workspace app version data for all OS platforms is displayed. You can view the version data for a specific OS platform by selecting the corresponding OS from the **Platform drop-down** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

When the type of host you're using doesn't support any particular metric, there's no icon appears for that particular metric. For example, no health information is available for System Center Virtual Machine Manager (SCVMM) hosts, AWS and CloudStack.

Continue to troubleshoot issues using these options (which are documented in the preceding sections):

- Control user machine power
- Prevent connections to machines

Monitor sessions

If a session becomes disconnected, it's still active and its applications continue to run. However, the user device is no longer communicating with the server.

ACTION	DESCRIPTION
View a user's currently connected machine or session	From the Activity Manager and User Details views, view the user's currently connected machine or session. Also, view a list of all machines and sessions to which this user has access. To access this list, click the session switcher icon in the user title bar. For more information, see Restore sessions.
View the total number of connected sessions across all delivery groups	From the Dashboard, in the **Sessions Connected** pane, view the total number of connected sessions across all delivery groups for the last 60 minutes. Then click the large total number, which opens the Filters view. Here, you can display graphical session data based on selected delivery groups and ranges and usage across delivery groups.
End idle sessions	The Sessions Filters view displays data related to all active sessions. You can filter the sessions that are based on Associated User, delivery group, Session State, and Idle Time greater than a threshold time period. From the filtered list, select sessions to log off or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION
	disconnect. For more information, see Troubleshoot applications.
View data over a longer period	On the **Trends** view, select the **Sessions** tab to drill down to more specific usage data. You can drill down data for connected and disconnected sessions over a longer period. You can view session totals from earlier than the last 60 minutes. To view this information, click **View historical trends**.

NOTE:

Consider that a user device is running on a legacy Virtual Delivery Agent (VDA), such as a VDA earlier than version 7, or a Linux VDA. In this case, Monitor can't display complete information about the session. Instead, it displays a message that the information isn't available.

Desktop Assignment Rules limitation: Studio allows assignment of multiple Desktop Assignment Rules (DAR) for different users or user groups to a single VDA in the delivery group. StoreFront™ displays the assigned desktop with the corresponding **Display Name** as per the DAR for the logged in user. However, Monitor does not support DARs and displays the assigned desktop using the delivery group name regardless of the logged in user. As a result, you can't map a specific desktop to a machine in Monitor.

You can map the assigned desktop that is displayed in StoreFront to the delivery group name that is displayed in Monitor. For mapping, use the following PowerShell command:

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

Run the preceding PowerShell command using the Remote PowerShell SDK as described in the blog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Disable the visibility of running applications in the Activity Manager

By default, the Activity Manager displays a list of all running applications for a user's session. All administrators who have access to the Activity Manager feature can view this information. For Delegated Administrator roles, this view includes Full Administrator, delivery group Administrator, and Help Desk Administrator.

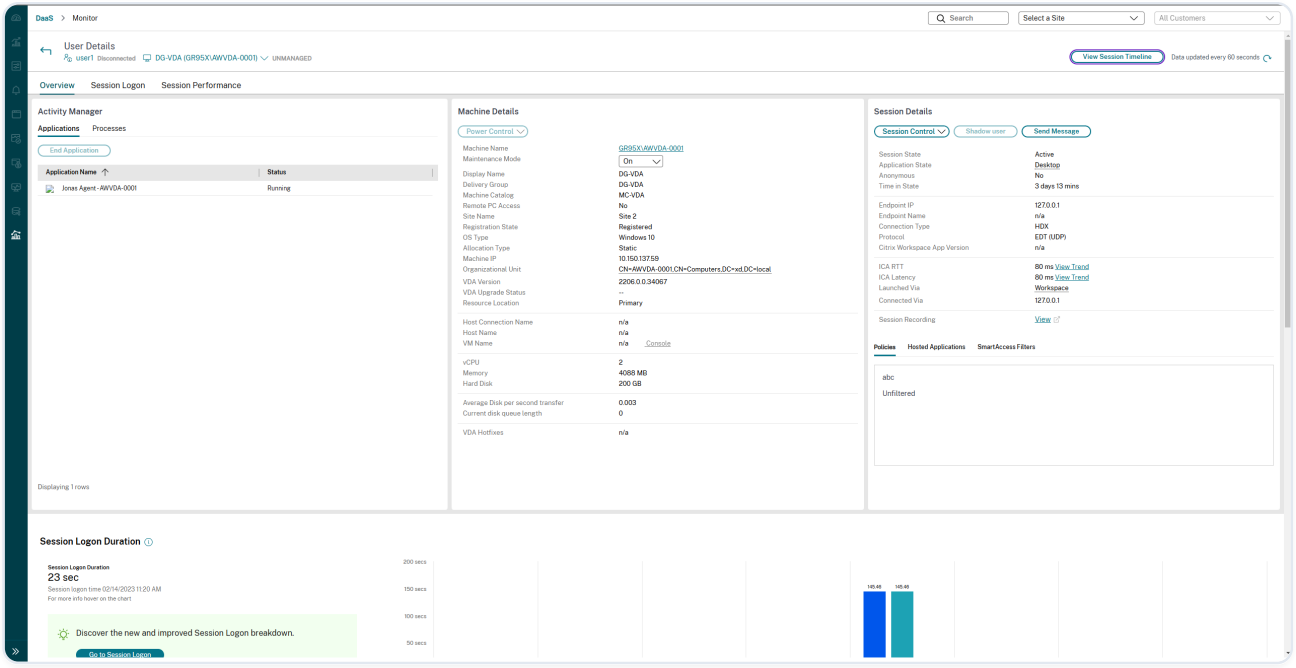
To protect the privacy of users and the applications that they're running, you can disable the **Applications** tab to list running applications. To do this activity, on the VDA modify the registry key at `HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed`. By default, the key is set to 1. Change the value to 0, which means the information isn't collected from the VDA and as such not displayed in the Activity Manager.

WARNING:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix® can't guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Access Citrix Analytics for Performance™ - Session Details

The Session Details page from Citrix Analytics for Performance can be accessed Monitor. Click **View Session Timeline** in the **Sessions Details** section of Activity Manager opens the Sessions Details page of Citrix Analytics for Performance within Monitor.

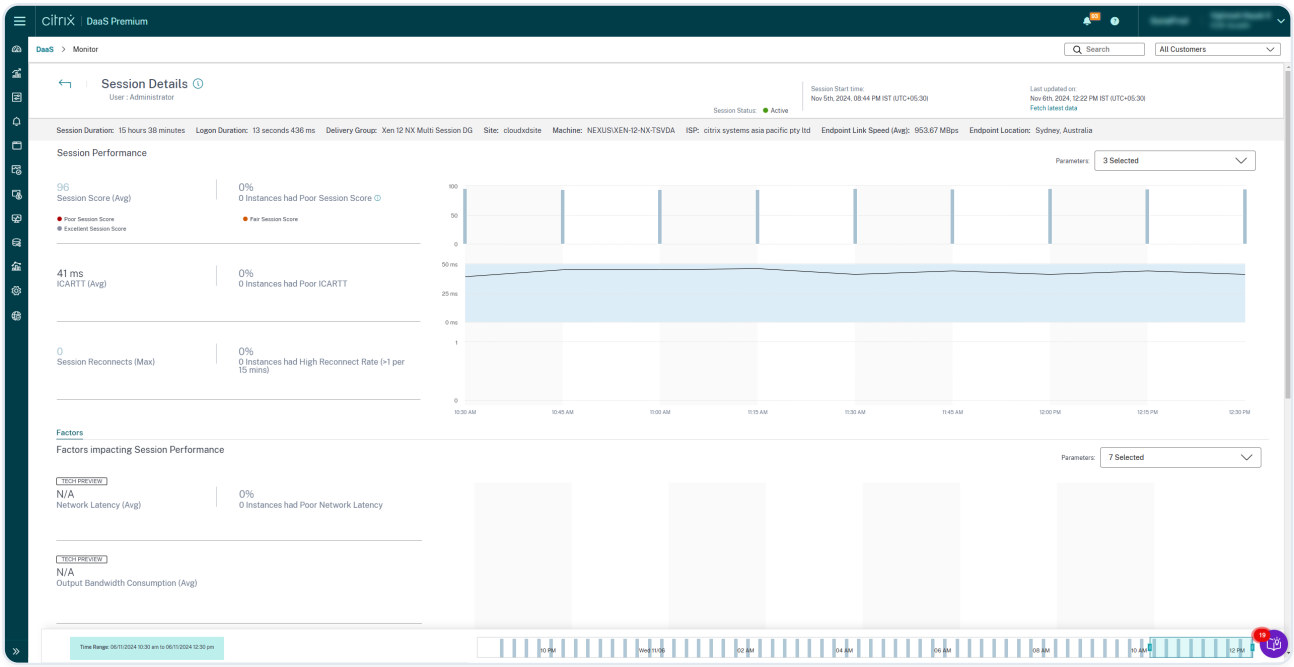


© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

This feature requires you to have a valid Citrix Analytics for Performance entitlement.

Session Details are available for sessions that are categorized as Excellent, Fair, or Poor Citrix Analytics for Performance. For more information about reasons why a session might not be categorized, see the Not Categorized article.



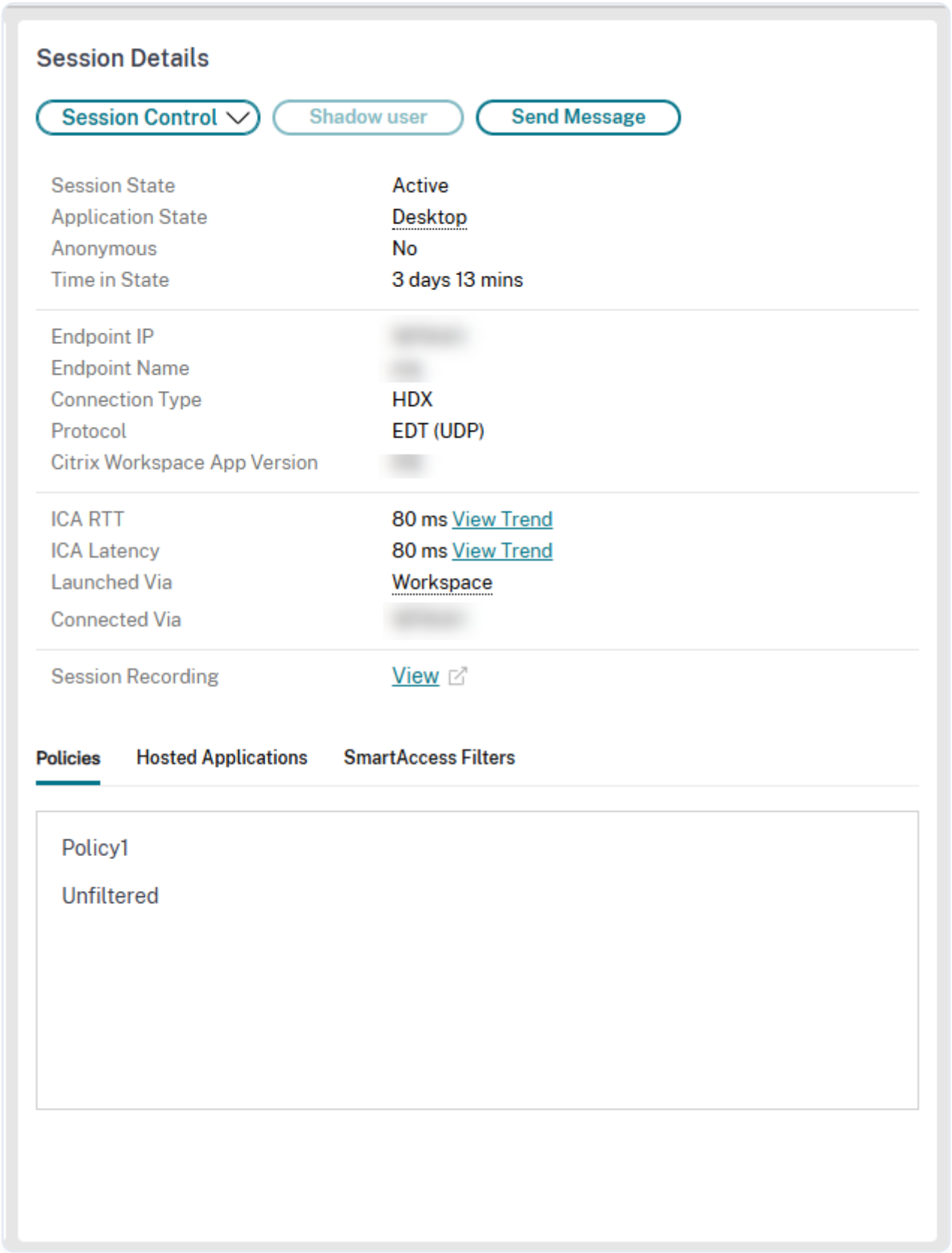
You can view a trend of the session experience for the session for up to the last three days. This trend view also includes the factors that contribute to the session experience. This information complements the live data available in Monitor, used by the help desk admin while troubleshooting issues related to session experience.

For more information about the Session Details page, see Session Details.

Session transport protocol

View the transport protocol in use for the HDX connection type for the current session in the **Session Details** panel. This information is available for sessions launched on VDAs Version 7.13 or later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Use the **Session Control** drop-down menu in the **Session Details** pane to log off or disconnect a session.

- For **HDX™** Connection type,
  - The Protocol is displayed as **UDP**, if EDT is used for the HDX connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - The Protocol is displayed as **TCP**, if TCP is used for the HDX connection.

- For **RDP** Connection type, the Protocol is displayed as **n/a**.

When adaptive transport is configured, the session transport protocol dynamically switches between EDT (over UDP) and TCP, based on the network conditions. If the HDX session can't be established using EDT, it falls back to the TCP protocol.

For more information about adaptive transport configuration, see Adaptive Transport.

Export reports

You can export trends data to generate regular usage and capacity management reports. Export supports PDF, Excel, and CSV report formats. Reports in PDF and Excel formats inculde trends represented as graphs and tables. Reports in CSV-format contain tabular data that you can use to generate views or to archive.

To export a report:

1. Go to the **Trends** tab.
2. Set filter criteria and time period and click **Apply**. The trend graph and table are populated with data.
3. Click **Export** and enter the name and format of the report.

Monitor generates the report based on the filter criteria that you select. If you change the filter criteria, click **Apply** before you click **Export**.

NOTE:

Export of a large amount of data causes a significant increase in memory and CPU consumption on the Monitor server, the Delivery Controller™, and the SQL servers. The supported number of concurrent export operations and the amount of data that can be exported is set to default limits to achieve optimal export performance.

Supported export limits

Exported PDF and Excel reports contain complete graphical charts for the selected filter criteria. However, tabular data in all report formats is truncated beyond the default limits on the number of rows or records in the table. The default number of records supported is defined based on the report format.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REPORT FORMAT	DEFAULT NUMBER OF RECORDS SUPPORTED
PDF	500
Excel	100,000
CSV	100,000 (10,000,000 in **Sessions** tab)

Error Handling

Errors that you might encounter during an Export operation:

- **Director has timed out:** This error can occur because of network issues or high resource usage on the Director server or with the Monitor Service.
- **Monitor has timed out:** This error can occur because of network issues or high resource usage with the Monitor Service or on the SQL server.
- **Max concurrent Export or Preview operations ongoing:** Only one instance of Export or Preview can run at a specific time. If you get the **Max concurrent Export or Preview operations ongoing** error, try the next operation again later.

Monitor hotfixes

To view the hotfixes installed on a specific machine VDA (physical or VM), choose the **Machine Details** view.

Control user machine power states

To control the state of the machines that you select in Monitor, use the Power Control options. These options are available for Single session OS machines, but might not be available for Multi-session OS machines.

NOTE:

This functionality isn't available for physical machines or machines using Remote PC Access.

COMMAND	FUNCTION
Restart	Performs an orderly (soft) shutdown of the VM and all running processes are halted individually before restarting the VM. For

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMMAND	FUNCTION
	example, select machines that appear in Monitor as "failed to start," and use this command to restart them.
Force Restart	Restarts the VM without first doing any shut-down procedure. This command works in the same way as unplugging a physical server and then plugging it back in and turning it back on.
Shut Down	Performs an orderly (soft) shutdown of the VM. All running processes are halted individually.
Force Shutdown	Shuts down the VM without first doing any shut-down procedure. This command works in the same way as unplugging a physical server. It might not always shut down all running processes, and you risk losing data if you shut down a VM in this way.
Suspend	Suspends a running VM in its current state and stores that state in a file on the default storage repository. This option allows you to shut down the VM's host server and later, after rebooting it, resume the VM, returning it to its original running state.
Resume	Resumes a suspended VM and restores its original running state.
Start	Starts a VM when it is off (also called a cold start).

If power control actions fail, hover the mouse over the alert, and a pop-up message appears with details about the failure.

Prevent connections to machines

Use maintenance mode to prevent new connections temporarily while the appropriate administrator performs maintenance tasks on the image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you enable maintenance mode on machines, no new connections are allowed until you disable it. If users are currently logged on, maintenance mode takes effect when all users are logged off. For users who do not log off, send a message informing them that machines are shut down at a certain time. You can use the power controls to force the machines to shut down.

1. Select the machine, such as from the User Details view, or a group of machines in the Filters view.
2. Select **Maintenance Mode**, and turn on the option.

If a user tries to connect to an assigned desktop while it is in maintenance mode, a message appears to indicate that the desktop is unavailable. No new connections can be made until you disable maintenance mode.

Application Analytics

The **Applications** tab displays application-based analytics in a single, consolidated view to help analyze and manage application performance efficiently. You can gain valuable insight into the health and usage information of all applications published on the site. It shows metrics such as the following:

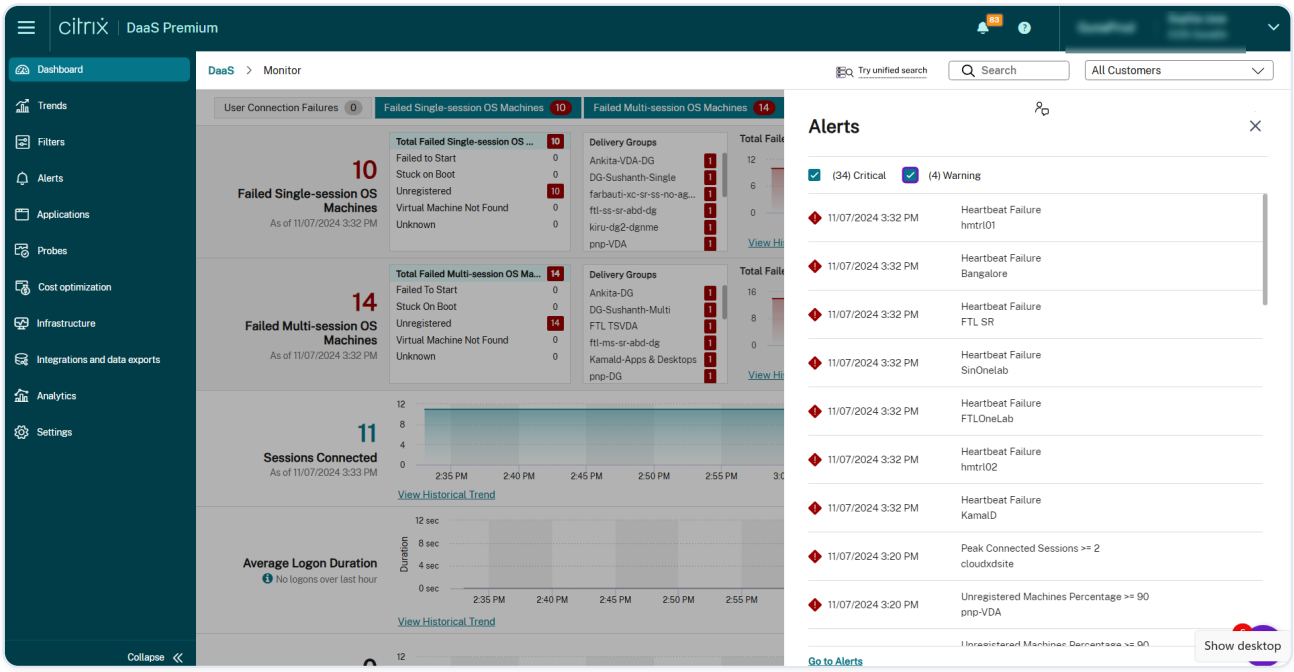
- Probe results
- Number of instances per application
- Faults and errors associated with the published applications

For more information, see the Application Analytics section in **Troubleshooting Applications**.

Alerts and notifications

Alerts are displayed in Monitor on the dashboard and other high level views with warning and critical alert symbols. Alerts update automatically every minute; you can also update alerts on demand.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



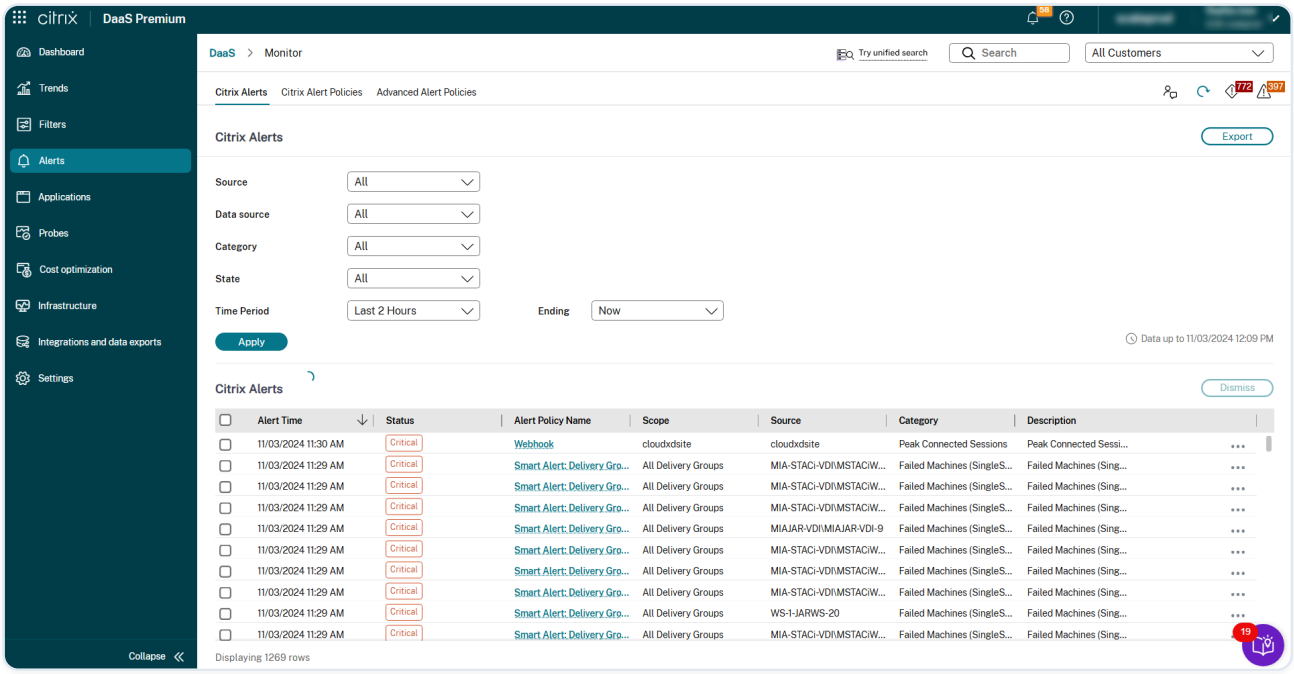
A warning alert (amber triangle) indicates that the warning threshold of a condition has been reached or exceeded.

A critical alert (red circle) shows that the critical threshold of a condition has been reached or exceeded.

You can view more detailed information on alerts by selecting an alert from the sidebar, clicking the **Go to Alerts** link at the bottom of the sidebar or by selecting **Alerts** from the top of the Monitor page.

In the Alerts view, you can filter and export alerts. For example, Failed Multi-session OS machines for a specific delivery group over the last month, or all alerts for a specific user. For more information, see Export reports.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix® alerts

Citrix alerts are the ones that originate from Citrix components. You can configure Citrix alerts within Monitor in **Alerts** \> **Citrix Alerts Policy**. As part of the configuration, you can set notifications to be sent by email to individuals and groups when alerts exceed the thresholds you have set up. For more information on setting up Citrix Alerts, see Create alerts policies.

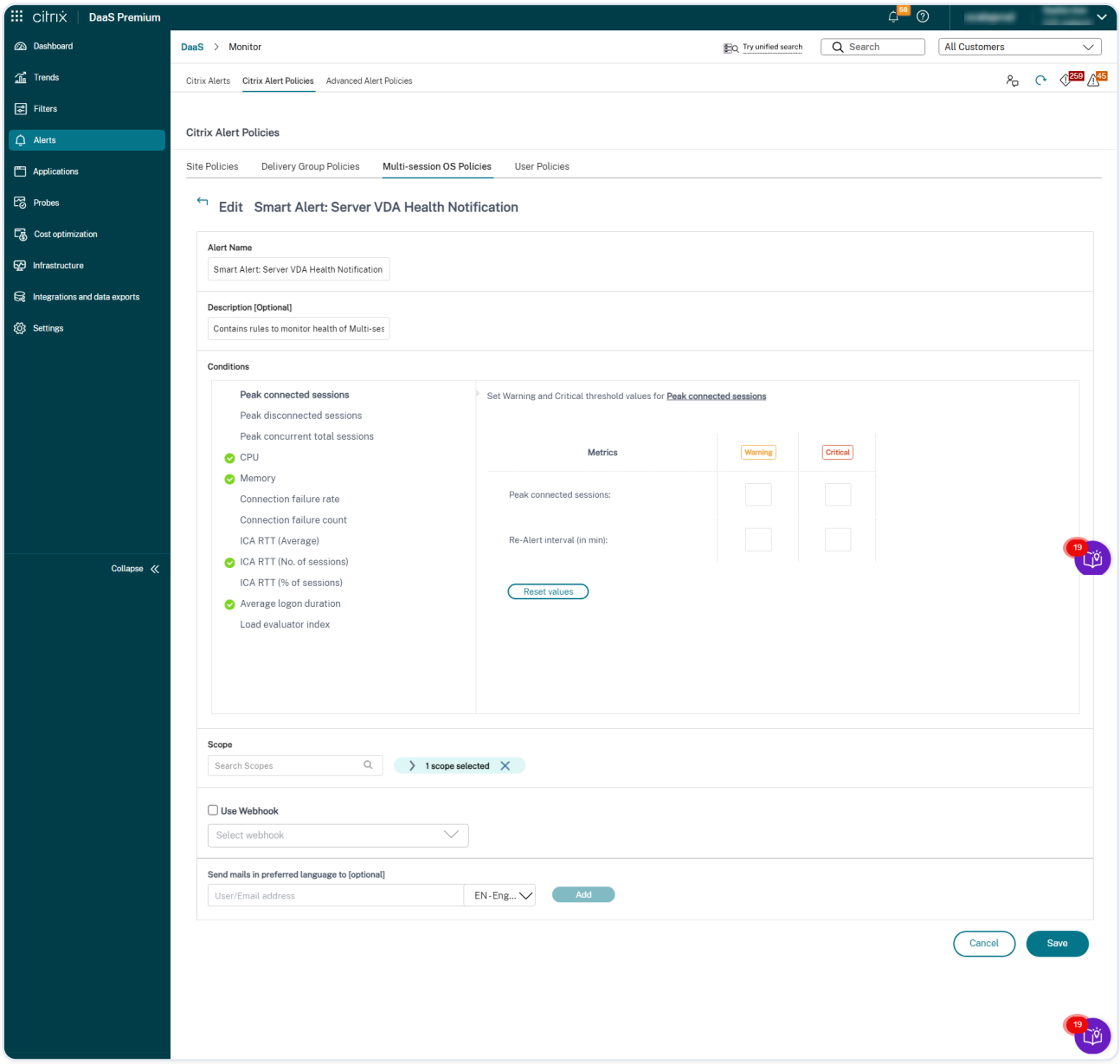
Smart alert policies

A set of built-in alert policies with predefined threshold values are available for delivery groups and Multi-session OS VDAs' scope. You can modify the threshold parameters of the built-in alert policies in **Alerts** \> **Citrix Alerts Policy**. These policies are created when there is at least one alert target -a delivery group or a Multi-session OS VDA defined in your site. Also, these built-in alerts are automatically added to a new delivery group or a Multi-session OS VDA.

Built-in alert policies are created only if no corresponding alert rules exist in the Monitor database.

For the threshold values of the built-in alert policies, see the Alerts policies conditions section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Advanced alert policies

The Proactive Notification and Alerting feature of the Monitor is enhanced to include a new alerting framework named **Advanced Alert Policies**. With this feature, you can create alerts by including granular details for each element or condition, thereby enhancing the control over the alerts scope. Currently, these policies include alerts for cost savings and infrastructure.

With the introduction of Advanced alert policies, which is a data source-driven alert you can use multi-condition scope filtering.

This feature helps you to reduce excessive alerts which might lead to reduced responsiveness or effectiveness in addressing important issues. This policy helps to measure effectiveness of alert policies and engagement from admins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can create an Advanced alert policy from the **Alerts** > **Advanced alert policy** > **Create Policy** section. You can select one of the following Data sources:

- Machines
- Provisioning Service
- StoreFront™

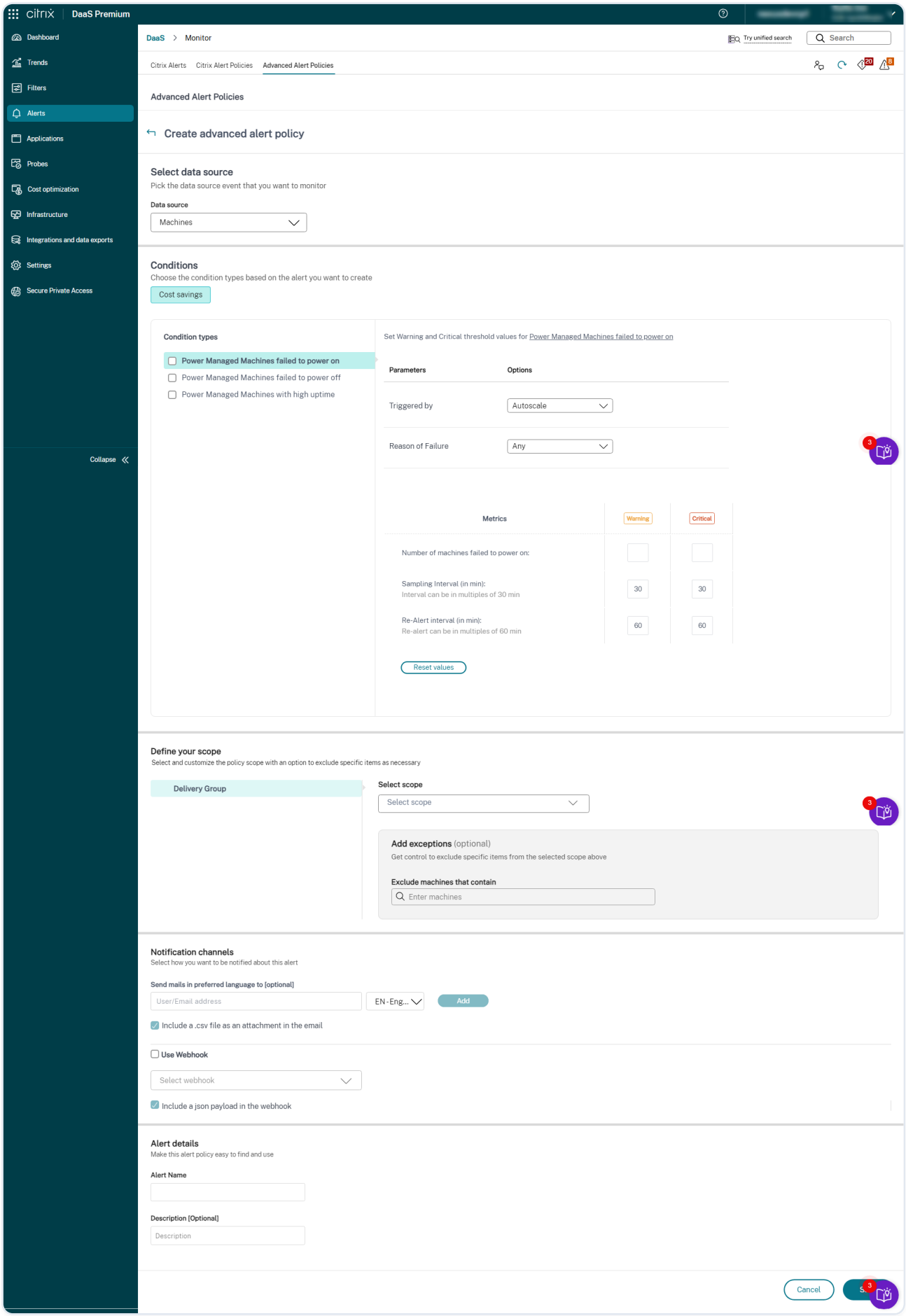
Alerts for cost savings

You can create alerts for cost savings which helps you to optimize cost. Currently, you can create alerts for machines.

To create alerts on Machines, do the following:

1. Click **Alerts** tab > **Advanced Alert Policies**. The **Advanced Alert Policies** page appears.
2. Click **Create Policy**. The **Create Advanced Alert Policies** section appears.
3. Select **Machines** from the Data source drop-down list. The Cost savings condition and corresponding condition types are displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Select the following condition types as required:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Power Managed Machines failed to power on**
- **Power Managed Machines failed to power off**
- **Power Managed Machines with high uptime**

2. Select the specific parameters and the corresponding options for each of the selected conditions.
3. Set the Warning and Critical metrics for the selected condition type:
    - For **Power Managed Machines with high uptime**:
        - Number of machines crossing uptime threshold
        - Re-alert interval (in min) interval can be minimum 60 min
    - For **Power Managed Machines failed to power on** and **Power Managed Machines failed to power off**:
        - Number of machines crossing uptime threshold
        - Sampling interval (in min) intervals can be multiples of 30 min
        - Re-alert interval (in min) re-alert can be multiples of 60 min
4. Schedule re-alert intervals for the selected alerts as needed.
5. Define the scope of the alert.
6. Set the notification channels. This can be email or Webhook.
    - You can select the following checkboxes:
        - **Include a JSON payload as an attachment in the webhook**
        - **Include a CSV file as an attachment in the email**
7. Enter the **Alert details** such as **Alert Name** and **Description** (optional).
8. Click **Save**. The alert is created.

Alerts for SPA Connection Latency

The Advanced Alert Policies framework supports proactive alerting for Secure Private Access (SPA) connectivity. Use this policy to detect and act on end-to-end latency affecting SPA user connections.

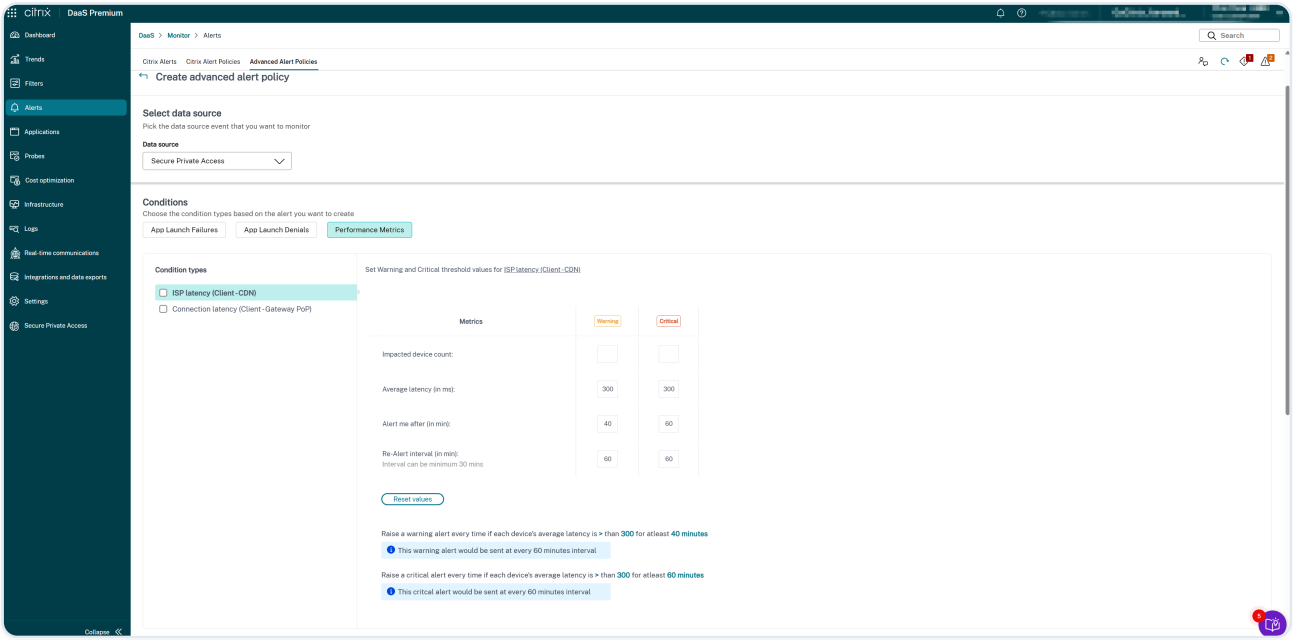
CONFIGURE SPA CONNECTION LATENCY ALERT

To create alerts for SPA Connection Latency, do the following:

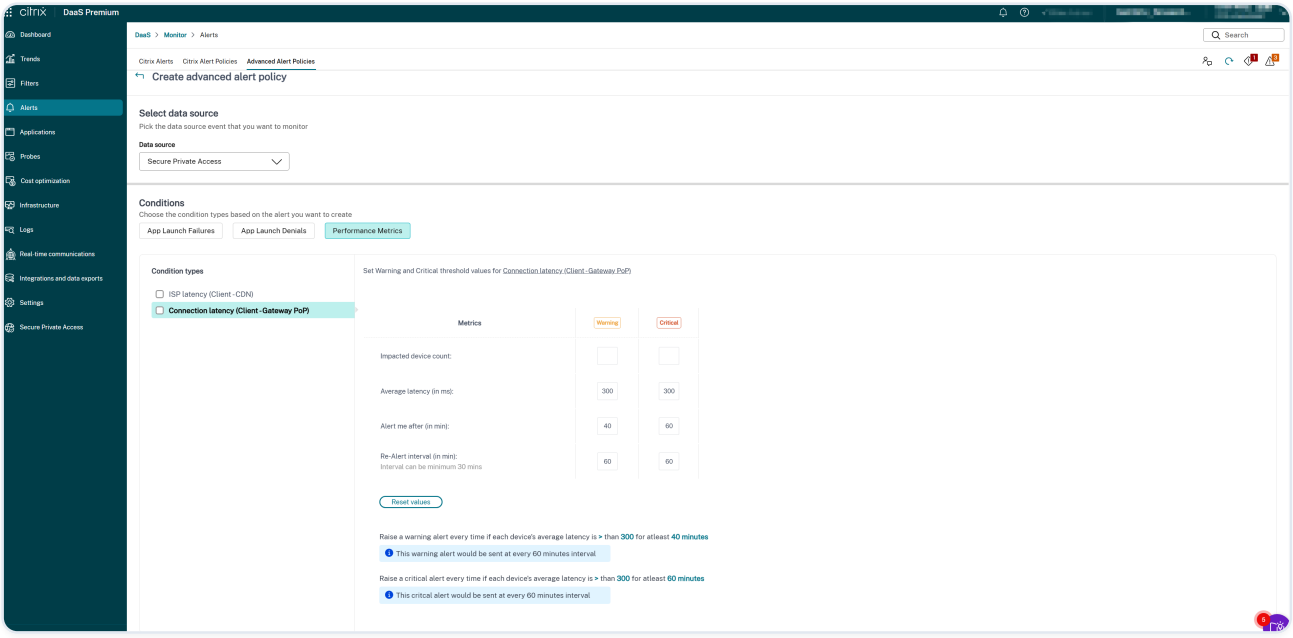
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Click **Alerts** tab > **Advanced Alert Policies**. The **Advanced Alert Policies** page appears.
2. Click **Create Policy**. The **Create Advanced Alert Policies** section appears.
3. Select **Secure Private Access** from the Data source drop-down list. The SPA Connection Latency condition is displayed.
4. Select the following metric types as required:
    - **ISP latency (Client → CDN)**
    - **Connection latency (Client → Gateway PoP)**

- ISP latency (Client → CDN)



- Connection latency (Client → Gateway PoP)



© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Select the specific parameters and the corresponding options for each of the selected metrics.
2. Set the Warning and Critical metrics for the selected condition type:
    - **Latency threshold (in ms)**: Set Warning (for example, 150–200 ms) and Critical (for example, 300–400 ms) values
    - **Impacted users (count)**: Number of users experiencing latency above threshold
    - **Sampling interval (in min)**: How often to evaluate latency (for example, 5–15 minutes)
    - **Re-alert interval (in min)**: Minimum 60 minutes recommended to avoid alert fatigue
3. Schedule re-alert intervals for the selected alerts as needed.
4. Define the scope of the alert. Select site, delivery group, or targeted subset.
5. Set the notification channels. This can be email or Webhook.
    - You can select the following checkboxes:
        - **Include a JSON payload as an attachment in the webhook**
        - **Include a CSV file as an attachment in the email**
6. Enter the **Alert details** such as **Alert Name** (for example, "SPA Connection Latency – PoP East") and **Description** (optional).
7. Click **Save**. The alert is created.

Recommendation:

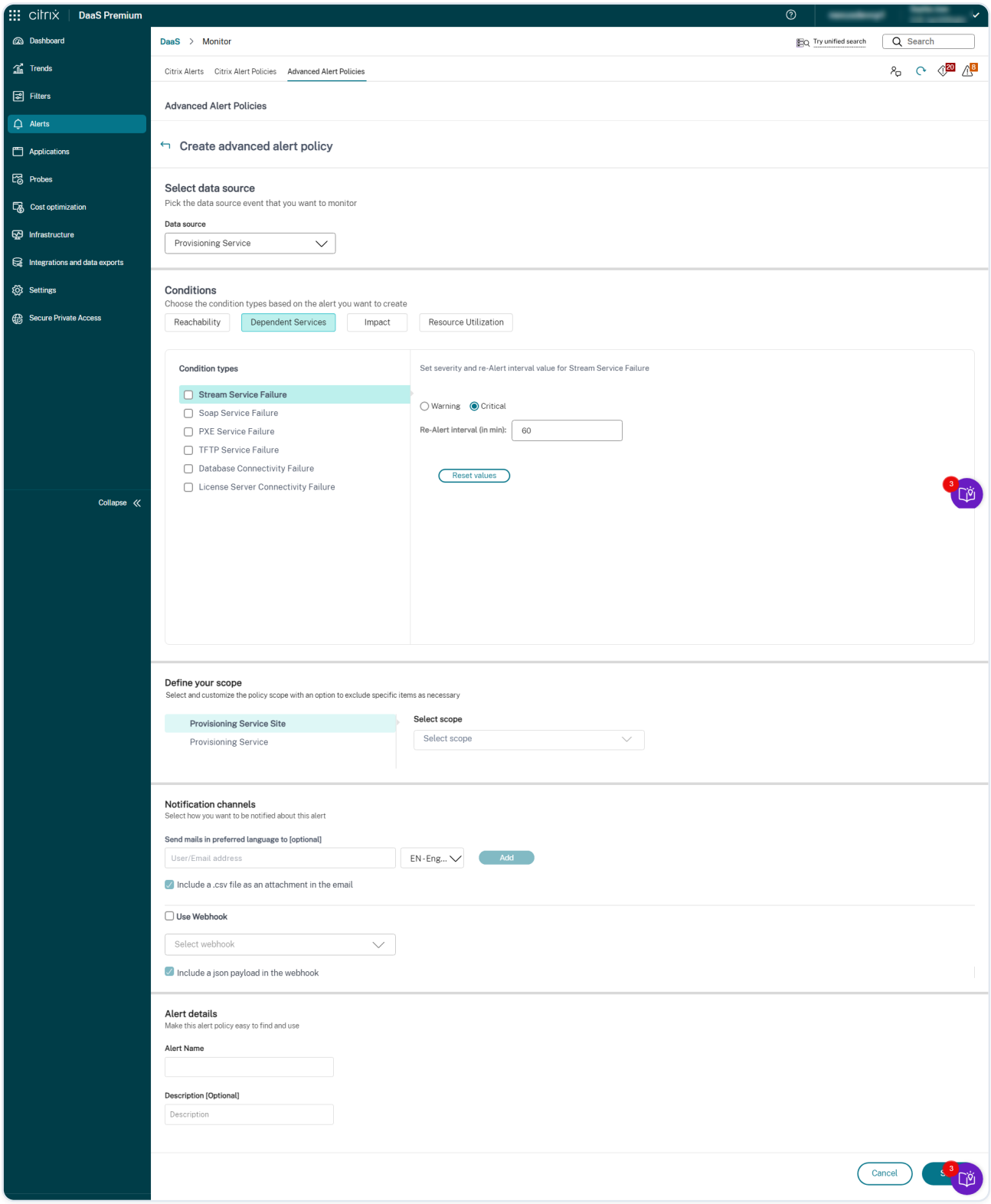
> For proactive alerting, adjust latency thresholds based on baseline measurements per region. Include webhook integration to route high-latency alerts into incident management for faster triage.

Infrastructure policies

You can create alerts to monitor the health of the following supported Citrix DaaS™ components:

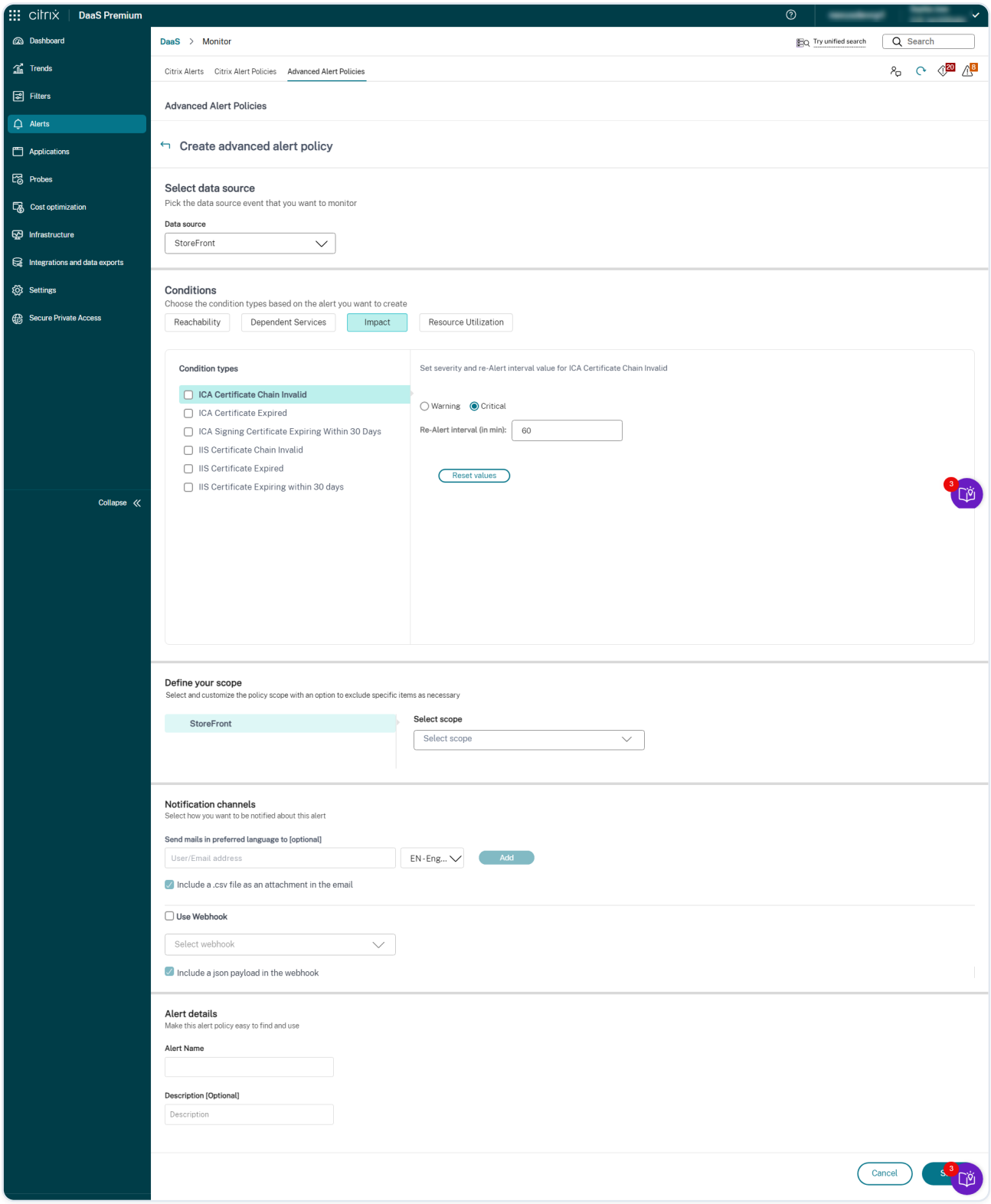
- Provisioning Service

© 1997–2026 Citrix Systems, Inc. All rights reserved.



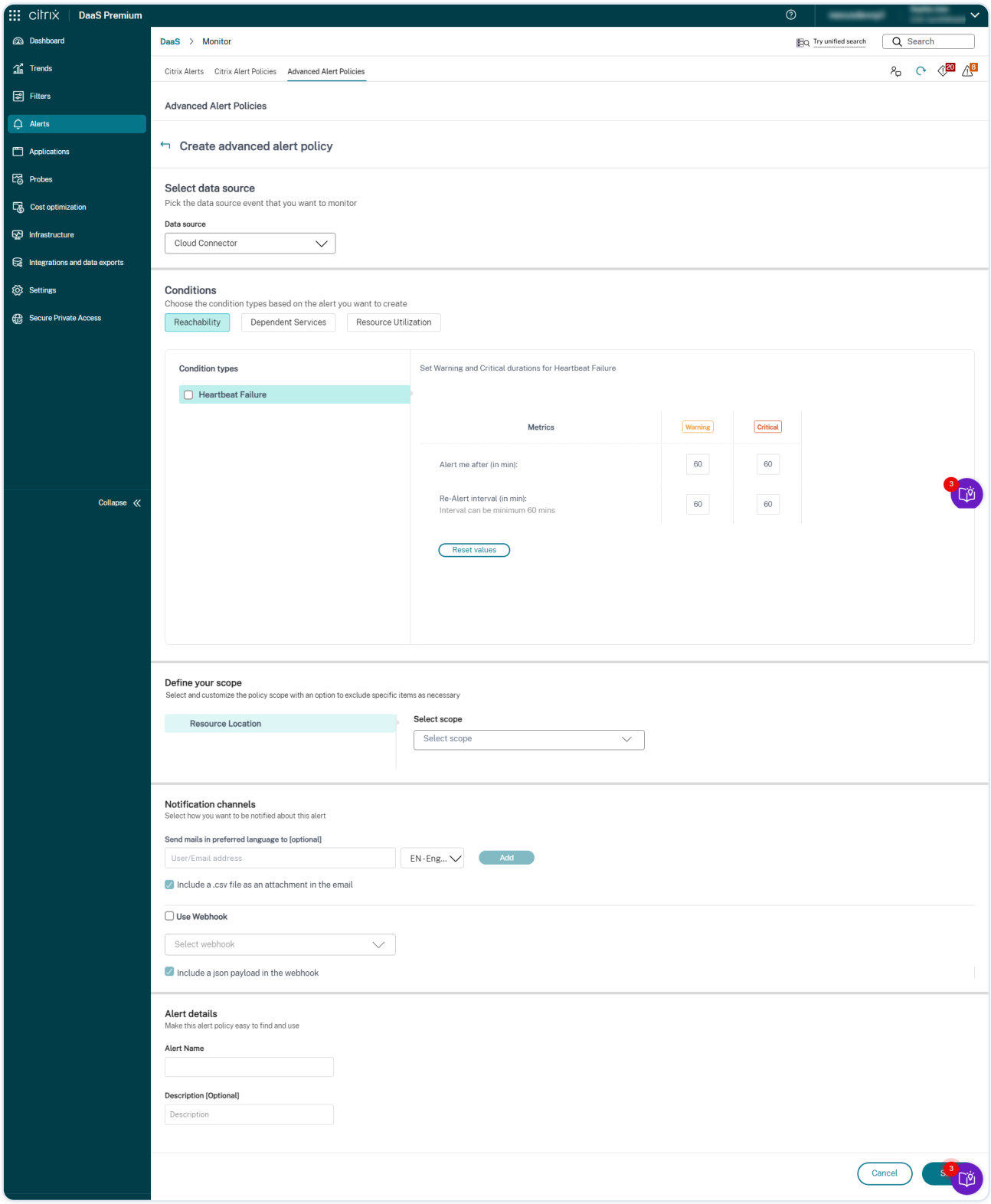
- StoreFront

© 1997–2026 Citrix Systems, Inc. All rights reserved.



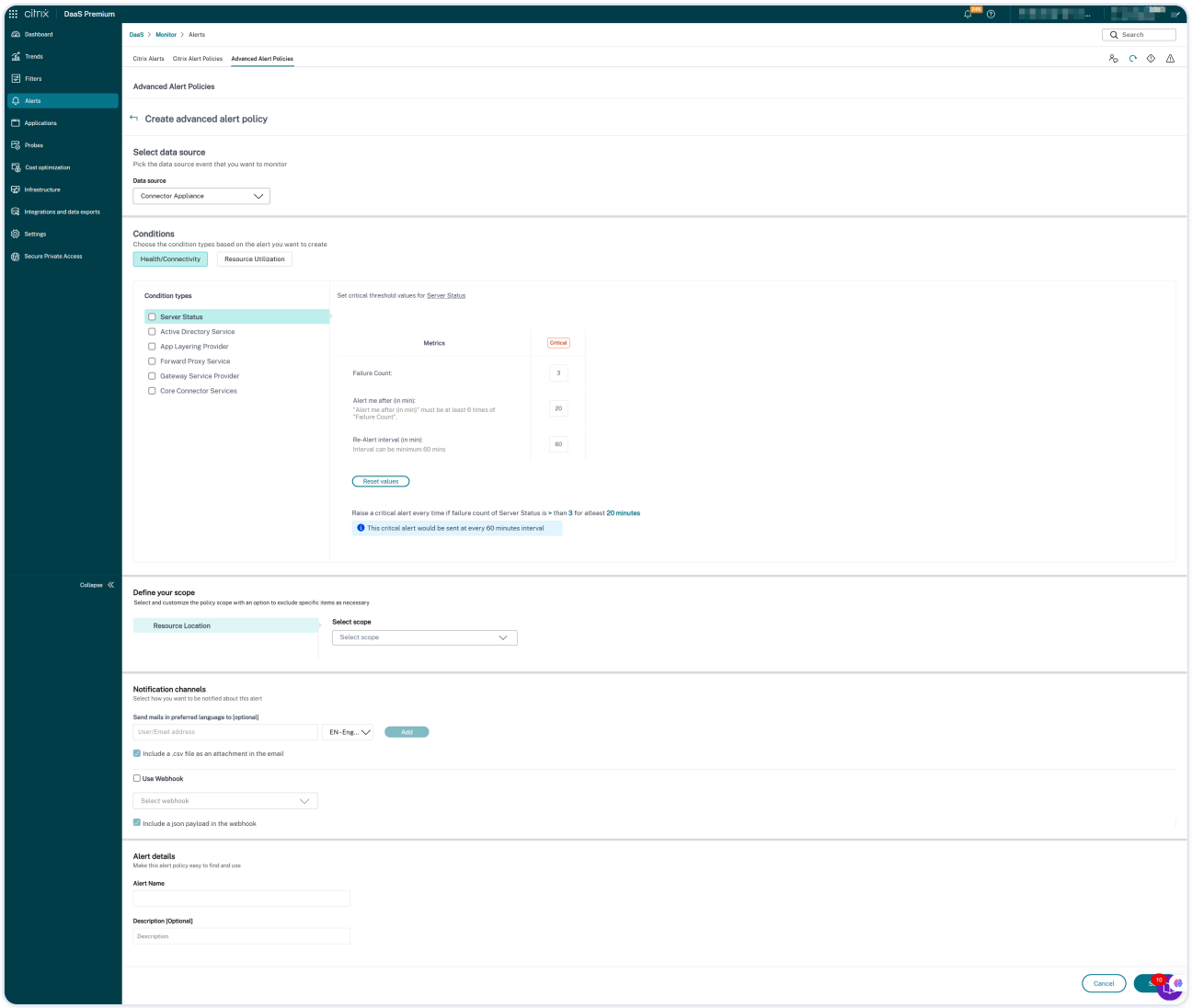
- Cloud Connector

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Connector Appliance

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Once the Infrastructure monitoring setup is completed, you can use the health data available in Monitor to configure alerts for any required component. Admins can set conditions, scopes, and notification mediums to receive important alerts through emails or a json payload through webhooks. The alerts raised are also available in the **Citrix Alerts** section for analysis and management.

As a part of the newly introduced Infrastructure policy, alert conditions are categorized into four sections as follows:

- Reachability
- Dependent services
- Impact
- Resource utilization

Conditions within each category can be set with the severity of **Critical** and **Warning** based on your organizational priorities. You can also schedule re-alert intervals for these alerts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can create an infrastructure policy from the **Alerts** > **Citrix Alert Policies** section. You can select the required category and then select the required conditions for the policy. For more information on how to create a policy, see Create alert policies. After the policy is created, you can edit, delete, or disable the policy on the Citrix Alerts page.

For more details on the conditions supported in each category and component, see the following:

- Provisioning health metrics
- StoreFront health metrics
- Cloud Connector health metrics
- Connector Appliance health metrics

The following data is received as an alert over email or on the Citrix Alert page:

FIELD	DESCRIPTION
Customer ID	The customer ID of the site.
Alert level	The possible values are Critical and Warning.
Target	The name of the machine for which the alert is triggered.
Time	The time when the alert is triggered.
Scope	The scope of the policy.
Policy	The name of the policy.
Description	The description of the issue for which the alert is triggered.

Define the scope of the policy

You can define the scope of your alert and add exceptions. The alert is generated only for the selected scope and the subscope excluded using add exceptions aren't included in alert generation. This feature helps you to create alerts on a granular level.

You can create notifications through emails or through webhook URLs. You can also select your preferred language in which you would like to receive alerts. You can also select an option to receive the alert parameters in a .CSV file attachment for email or in a json payload through a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

webhook URL. The attachment includes details of the required parameters. For more information, see Enhancements on alert content.

The following data is received as an alert over email or on the **Citrix Alerts** page:

FIELD	DESCRIPTION
Customer ID	The customer ID of the site.
Alert level	This value is the predefined value set for each alert condition. The possible values are Critical and Warning.
Condition	This value is the condition set while creating the policy. For example, the number of unregistered machines is equal to or more than 20.
Target	The name of the delivery group or site for which the alert is triggered.
Site	The name of the site.
Scope	The scope of the policy. This value includes subscope also.
Policy	The name of the policy.
Description	The description of the issue for which the alert is triggered.

How to create an Advanced alert policy using a PowerShell script?

PowerShell script to create an alert policy:

```
asnp Citrix.Monitor.*

# Add Parameters

$timeSpan = New-TimeSpan -Seconds 30

$alertThreshold = 1

$alarmThreshold = 2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
# Add Target UID's

$targetIds = @()

$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"

# Add email addresses

$emailaddress = @()

$emailaddress += "loki@abc.com"

# Create new policy

$policy = New-MonitorNotificationPolicy -Name
"FailedMachinePercentageAlertCreationViaPowershell" -Description "Policy
created to test urm" -Enabled $true
```

REPLACE THE FOLLOWING LINE WITH THE CORRECT CONDITION FOR FAILEDMACHINEPERCENTAGE

```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
FailedMachinePercentage -AlertThreshold $alertThreshold -AlarmThreshold
$alarmThreshold -AlertRenotification $timeSpan -AlarmRenotification
$timeSpan



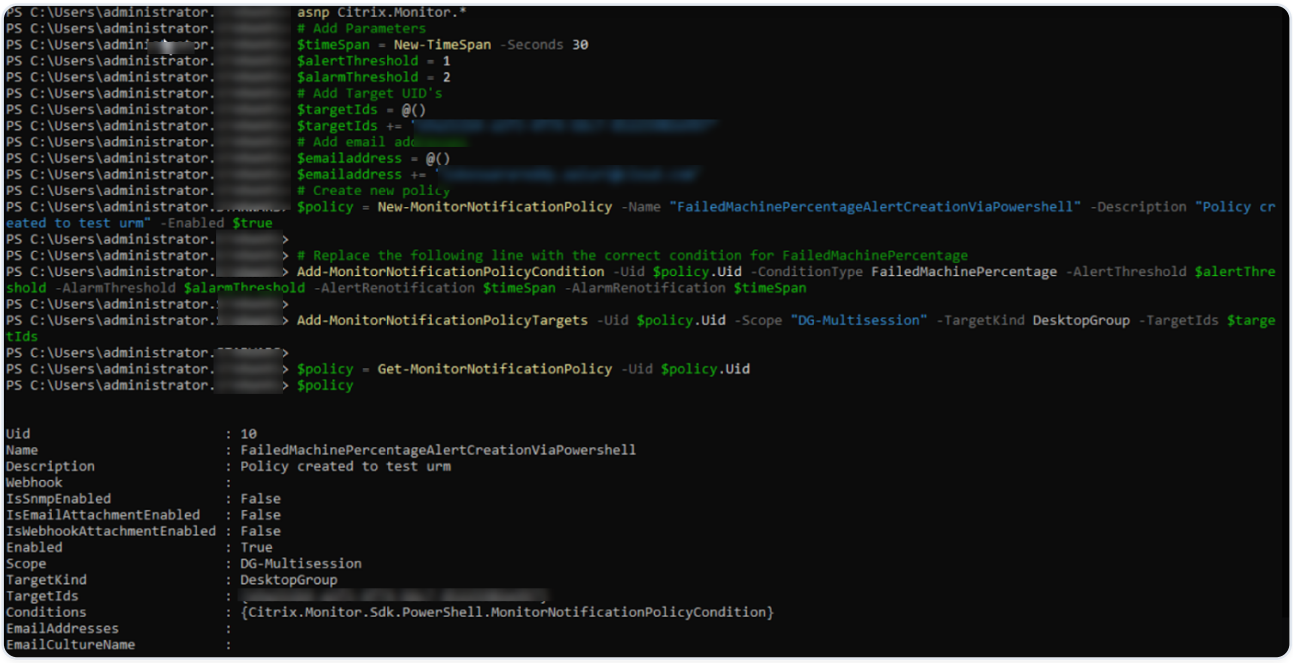
Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
Multisession" -TargetKind DesktopGroup -TargetIds $targetIds



$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid

$policy
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.



From the preceding image, you can see that the policy is created and Uid is 10.

TO ADD EMAIL TO CONFIGURATION

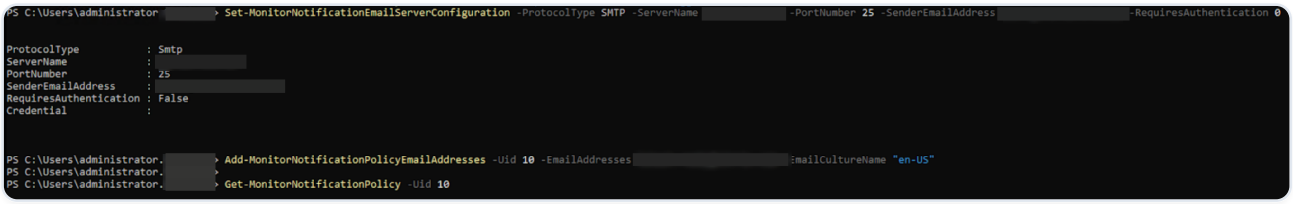
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP
-ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80
-SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

TO ADD EMAIL TO POLICY

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid
-EmailAddresses $emailaddress -EmailCultureName "en-US"
```

Sample script to add email:

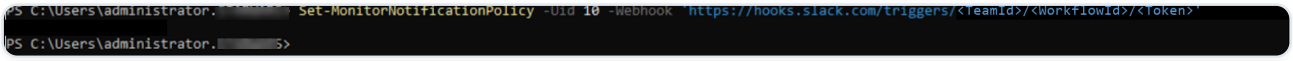
```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
$emailaddress -EmailCultureName "en-US"
```



TO ADD WEBHOOK URL TO POLICY

```
Set-MonitorNotificationPolicy –Uid $polcy.Uid –Webhook 'URL'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

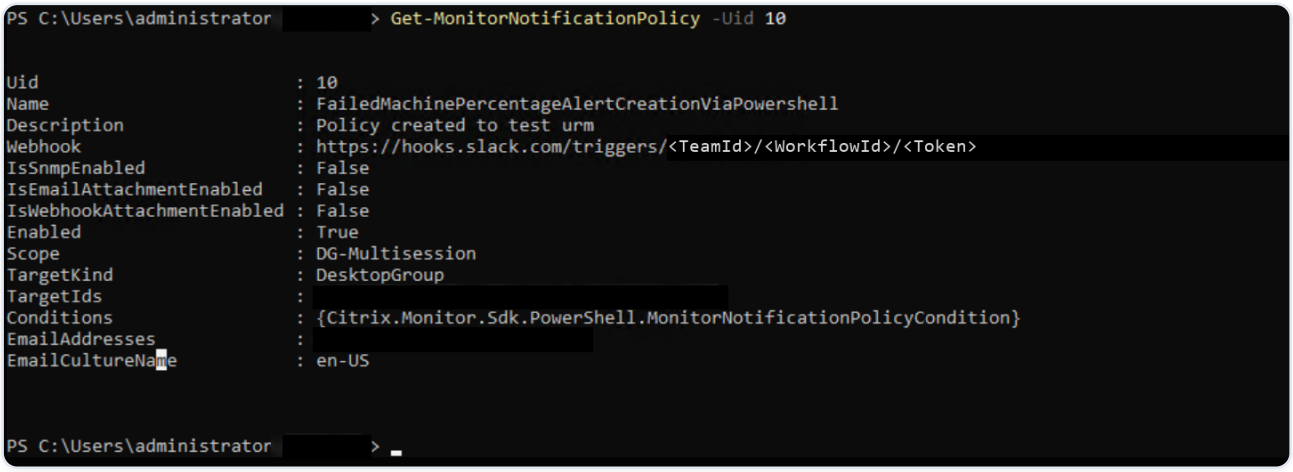


Sample scipt to add webhook URL:

```
Set-MonitorNotificationPolicy –Uid 10  –Webhook  'https://hooks.slack.com/triggers/<TeamId>/<WorkflowId>/<Token>'
```

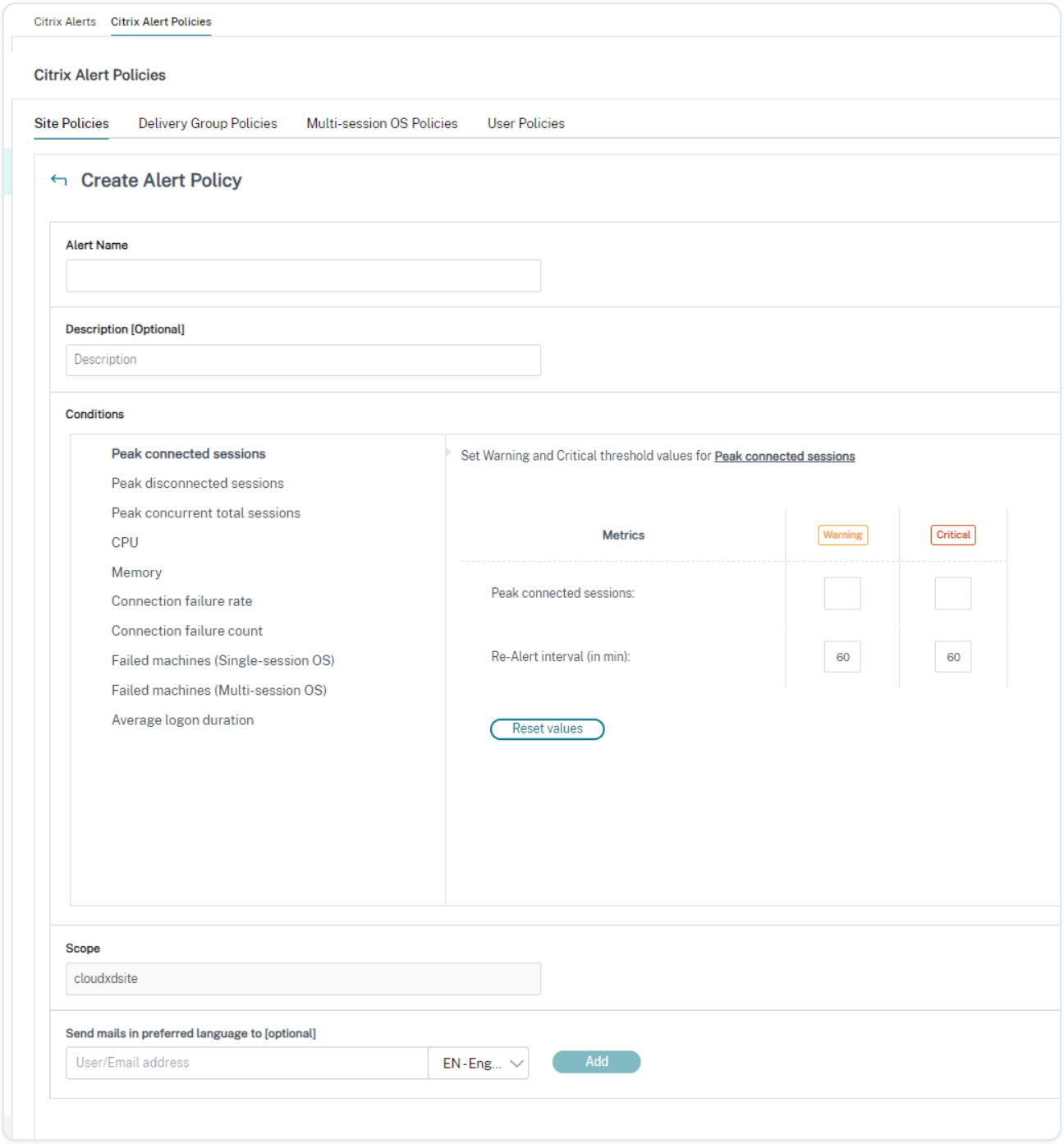
GET CREATED POLICY DETAILS

```
Get-MonitorNotificationPolicy -Uid 10
```



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create alerts policies



To create alerts policy, for example, to generate an alert when a specific set of session count criteria are met:

1. Go to **Alerts** \> **Citrix Alerts Policy** and select, for example, Multi-session OS Policy.
2. Click **Create**.
3. Name and describe the policy, then set the conditions that have to be met for the alert to be triggered. For example, specify Warning and Critical counts for Peak Connected Sessions, Peak Disconnected Sessions, and Peak Concurrent Total Sessions. Warning values must not be greater than Critical values. For more information, see Alerts policies conditions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Set the Re-alert interval. If the conditions for the alert are still met, the alert is triggered again at this time interval and, if set up in the alert policy, an email notification is generated. A dismissed alert does not generate an email notification at the re-alert interval.
5. Set the Scope. For example, set for a specific delivery group.
6. In Notification preferences, specify who should be notified by email when the alert is triggered. Email notifications are sent via SendGrid. Ensure that the email address `donotreplynotifications@citrix.com` is white-listed in your email setup.
7. Click **Save**.

Creating a policy with 20 or more delivery groups defined in the Scope might take approximately 30 seconds to complete the configuration. A spinner is displayed during this time.

Creating more than 50 policies for up to 20 unique delivery groups (1000 delivery group targets in total) might result in an increase in response time (over 5 seconds).

Moving a machine containing active sessions from one delivery group to another might trigger erroneous delivery group alerts that are defined using machine parameters.

NOTE:

After you delete an alert policy, it might take up to 30 minutes for the alert notifications generated by the policy to stop.

Enhancements on alert content

The alerting feature of the Monitor is enhanced to include a CSV attachment and a JSON payload. With this enhancement, you can get alert details in a CSV attachment over email or as a JSON payload if there is a webhook. Using this CSV attachment or JSON payload, you can receive enriched content at a detailed level, aiding in the quick identification and resolution of issues.

Currently, this enhancement is available only on the following alerts:

- Machine uptime
- Failed power on actions
- Failed power off actions
- Unregistered machines (%)

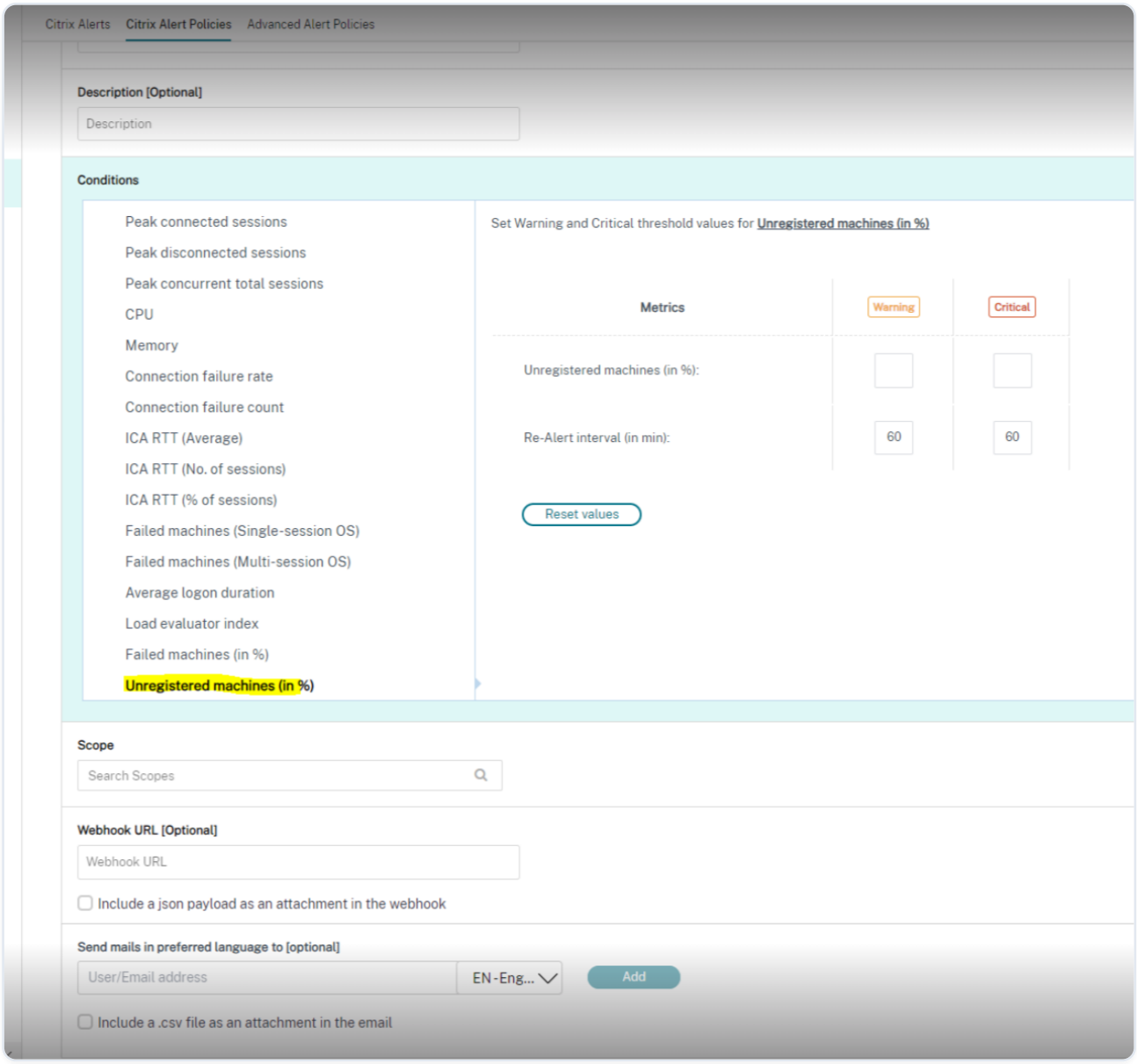
To use this feature, navigate to the alert and select the following checkboxes:

- **Include a json payload as an attachment in the webhook**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

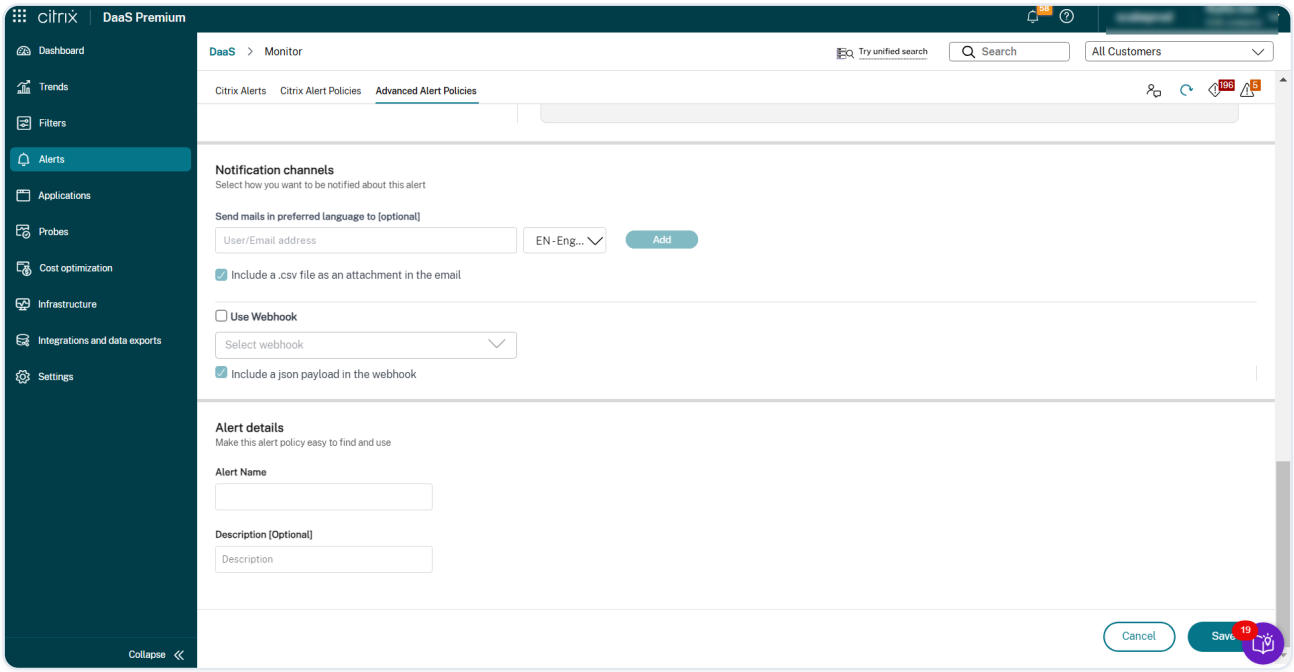
- **Include a csv file as an attachment in the email**

The following is a screenshot from the **Citrix Alert Policies** section:



Here is a screenshot from **Advanced Alert Policies** section:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



CSV ATTACHMENT

The following table provides columns of the .CSV attachment for all supported alerts:

COLUMN	APPLICABLE ALERT
Machine Name, IP Address, and Delivery Group Name	Machine uptime, Failed power off action and Failed power on action, and Unregistered machines (%)
Current Registration State, Failure Date, Fault State, and Lifecycle State	Unregistered machine (%)
Last Power Action Failure Reason, Last Power Action Triggered By, Last Power Action Type, and Last Power Action Completed Date	Failed power off action and Failed power on action
Power State, Powered On Date, and Total Uptime In Minutes	Machine uptime

WEBHOOK PAYLOAD

Unregistered Machine Percentage Alert

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
\"Condition\":\"Unregistered machines (in %)\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"CurrentRegistrationState\":\"Unregistered\",
\"FailureDate\":\"<Date of Failure>\",\"FaultState\":\"<Fault State of the
Machine>\",\"LifecycleState\":\"<Lifecycle state of the Machine>\"},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"CurrentRegistrationState\":\"Unregistered\",\"FailureDate\":\"<Date of
Failure>\",\"FaultState\":\"<Fault State of the Machine>\",
\"LifecycleState\":\"<Lifecycle state of the Machine>\"}]}"

}
```

Failed power on actions Alert

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOn Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of the
DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

Failed power off actions Alert

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOff Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IPV4 Address of the Machine>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IPV4 Address of the Machine>\",\"DeliveryGroupName\":
\"<Name of the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"

}
```

Machine Uptime alert

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Machine Uptime Alert\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"PowerState\":\"<On/Off>\",\"PoweredOnDate\":
\"2024-05-15T15:04:27.723\",\"TotalUptimeInMinutes\":180},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",\"PowerState\":
\"<ON/OFF>\",\"PoweredOnDate\":\"2024-05-15T15:04:27.723\",
\"TotalUptimeInMinutes\":\"<Uptime Duration>\"}]}"

}
```

Alerts policies conditions

Find below the alert categories, recommended actions to mitigate the alert, and built-in policy conditions if defined. The built-in alert policies are defined for alert and realert intervals of 60 minutes.

Peak Connected Sessions

- Check the Monitor Session Trends view for peak connected sessions.
- Check to ensure that there is enough capacity to accommodate the session load.
- Add new machines if needed

Peak Disconnected Sessions

- Check the Monitor Session Trends view for peak disconnected sessions.
- Check to ensure that there is enough capacity to accommodate session load.
- Add new machines if needed.
- Log off disconnected sessions if needed

Peak Concurrent Total Sessions

- Check the Monitor Session Trends view in Monitor for peak concurrent sessions.
- Check to ensure that there is enough capacity to accommodate session load.
- Add new machines if needed.
- Log off disconnected sessions if needed

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CPU

Percentage of CPU usage indicates the overall CPU consumption on the VDA, including that of the processes. You can get more insight into the CPU utilization by individual processes from the **Machine details** page of the corresponding VDA.

- Go to **Machine Details > View Historical Utilization > Top 10 Processes**, identify the processes consuming the CPU. Ensure that the process monitoring policy is enabled to initiate collection of process level resource usage statistics.
- End the process if necessary.
- Ending the process causes unsaved data to be lost.
- If all is working as expected, add more CPU resources in the future.

> **NOTE:**
>
> The policy setting, **Enable resource monitoring** is allowed by default for the monitoring of CPU and memory performance counters on machines with VDAs. If this policy setting is disabled, alerts with CPU and memory conditions are not triggered. For more information, see Monitoring policy settings.

Smart policy conditions:

- **Scope:** Delivery group, Multi-session OS scope
- **Threshold values:** Warning - 80%, Critical - 90%

Memory

Percentage of Memory usage indicates the overall memory consumption on the VDA, including that of the processes. You can get more insight into the memory usage by individual processes from the **Machine details** page of the corresponding VDA.

- Go to **Machine Details > View Historical Utilization > Top 10 Processes**, identify the processes consuming memory. Ensure that the process monitoring policy is enabled to initiate collection of process level resource usage statistics.
- End the process if necessary.
- Ending the process causes unsaved data to be lost.
- If all is working as expected, add more memory in the future.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The policy setting **Enable resource monitoring**, is allowed by default for the monitoring of CPU and memory performance counters on machines with VDAs. If this policy setting is disabled, alerts with CPU and memory conditions aren't triggered. For more information, see Monitoring policy settings.

Smart policy conditions:

- **Scope:** Delivery group, Multi-session OS scope
- **Threshold values:** Warning - 80%, Critical - 90%

Connection Failure Rate

Percentage of connection failures over the last hour.

- Calculated based on the total failures to total connections attempted.
- Check the Monitor Connection Failures Trends view for events logged from the Configuration log.
- Determine if applications or desktops are reachable.

Connection Failure Count

Number of connection failures over the last hour.

- Check the Monitor Connection Failures Trends view for events logged from the Configuration log.
- Determine if applications or desktops are reachable.

ICA® RTT (Average)

Average ICA round-trip time.

- Check Citrix ADM for a breakdown of the ICA RTT to determine the root cause. For more information, see the Citrix ADM documentation.
- If Citrix ADM is not available, check the Monitor User Details view for the ICA RTT and Latency, and determine if it is a network problem or an issue with applications or desktops.

ICA RTT (No. of Sessions)

Number of sessions that exceed the threshold ICA round-trip time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Check Citrix ADM for the number of sessions with high ICA RTT. For more information, see the Citrix ADM documentation.
- If Citrix ADM isn't available, contact the network team to determine the root cause.

  Smart policy conditions:

  - **Scope:** Delivery group, Multi-session OS scope
  - **Threshold values:** Warning - 300 ms for 5 or more sessions, Critical - 400 ms for 10 or more sessions

ICA RTT (% of Sessions)

Percentage of sessions that exceed the average ICA round-trip time.

- Check Citrix ADM for the number of sessions with high ICA RTT. For more information, see the Citrix ADM documentation.
- If Citrix ADM is not available, contact the network team to determine the root cause.

ICA RTT (User)

ICA round-trip time that is applied to sessions launched by the specified user. The alert is triggered if ICA RTT is greater than the threshold in at least one session.

Failed Machines (Single session OS)

Number of failed Single session OS machines. Failures can occur for various reasons as shown in the Monitor Dashboard and Filters views.

- Run Citrix Scout diagnostics to determine the root cause. For more information, see Troubleshoot user issues.

  Smart policy conditions:

  - **Scope:** Delivery group scope
  - **Threshold values:** Warning - 1, Critical - 2

Failed Machines (Multi-session OS)

Number of failed Multi-session OS machines. Failures can occur for various reasons as shown in the Monitor Dashboard and Filters views.

- Run Citrix Scout diagnostics to determine the root cause.

  Smart policy conditions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Scope:** Delivery group, Multi-session OS scope
- **Threshold values:** Warning - 1, Critical - 2

Failed Machines (in %)

The percentage of failed single-session and multi-session OS machines in a delivery group calculated based on the number of failed machines. This alert condition allows you to configure alert thresholds as a percentage of failed machines in a delivery group and is calculated every 30 seconds. Failures can occur for various reasons as shown in the Monitor Dashboard and Filters views. Run Citrix Scout diagnostics to determine the root cause. For more information, see Troubleshoot user issues.

Failed power on action and Failed Power off action

Number of failed power on actions and number of failed power off actions in a delivery group calculated based on number of **Power Managed Machines** that failed to power on or off. This alert condition allows you to configure alert thresholds as the number of **Power Managed Machines** that failed to power on or off in a delivery group and is calculated every 30 minutes.

Admin can configure the following parameters for these alerts in the Advanced alert policy:

- Triggered By: What triggered the power action
- Reason Of failure: Why the action failed
- Threshold: Threshold number of machines that failed power action to trigger the policy
- Sampling interval: The interval In which the failed power action has to be checked
- Re-alert interval: After how much time the alert must be re-sent

Failures can occur for various reasons as shown in the Monitor Dashboard and Filters views. Run Citrix Scout diagnostics to determine the root cause. For more information, see Troubleshoot user issues.

Unregistered machines (in %)

A machine is considered unregistered, when a machine becomes unstable due to a restart or when there is a communication problem between the delivery controller™ and the virtual machines. The **Unregistered machines (in %)** is the percentage of unregistered single-session and multi-session OS machines in a delivery group calculated based on the number of unregistered machines. This alert condition allows you to configure warning and critical threshold values as a percentage of unregistered machines in a delivery group. You can set an interval for re-alert. You can also add an email to get a notification when the conditions are met for **Unregistered Machines (in %)**. When the critical or warning threshold value is exceeded, alerts and emails are generated. You can view

© 1997–2026 Citrix Systems, Inc. All rights reserved.

alerts under **Citrix Alerts**. You can filter it by **Unregistered Machines (in %)** category and for the required state and time.

NOTE:

The critical value must be greater than the warning value.

Policy conditions:

- **Scope**: Single-session OS, and Multi-session OS Delivery group
- **Threshold values**: Warning and Critical

Machine uptime alert

Machine uptime in a delivery group is calculated based on the number of hours per day, hours per week, or hours per month for a machine that is turned on in a delivery group. This alert condition allows you to configure alert thresholds as the hours a machine is turned on in a delivery group. The machine uptime alerts works as follows in case of:

- Hours per day - You can specify the number of hours a machine is turned on for a day and is calculated every 30 minutes. The maximum number of hours per day that you can set is 24 hours.
- Hours per week - You can specify the number of hours a machine is turned on for a week and is calculated every six hours. The maximum number of hours per week that you can set is 168 hours.
- Hours per month - You can specify the number of hours a machine is turned on for a month and is calculated once every day. The maximum number of hours per month is 720 hours. The minimum re-alert interval value that you can set is 60 minutes. You can enter the number of machines that cross the machine uptime threshold value under the Warning and Critical alerts section. You can also add exceptions for any machines.

For example, if there are five delivery groups added for this alert and if in the first delivery group and fourth delivery group, the number of machines crosses the warning or critical threshold values, the alert is triggered separately for the first delivery group and for the fourth delivery group.

This alert helps the admins to analyze the uptime of the machines and based on this analysis the admins can help in optimizing the cost. You can also receive alert details in a CSV attachment in an email or through a JSON payload in case of a webhook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Average Logon Duration

Average logon duration for logons that occurred over the last hour.

- Check the Monitor Dashboard to get up-to-date metrics regarding the logon duration. A large number of users logging in during a short timeframe can increase the logon duration.
- Check the baseline and break down of the logons to narrow down the cause. For more information, see Diagnose user logon issues.

  Smart policy conditions:

  - **Scope:** Delivery group, Multi-session OS scope
  - **Threshold values:** Warning - 45 seconds, Critical - 60 seconds

Logon Duration (User)

Logon duration for logons for the specified user that occurred over the last hour.

Load Evaluator Index

Value of the Load Evaluator Index over the last 5 minutes.

- Check Monitor for Multi-session OS Machines that might have a peak load (Max load). View both Dashboard (failures) and Trends Load Evaluator Index report.

  Smart policy conditions:

  - **Scope:** Delivery group, Multi-session OS scope
  - **Threshold values:** Warning - 80%, Critical - 90%

Configure alerts policies with webhooks

Apart from email notifications, you can configure alerts policies with webhooks.

Note: This feature requires Delivery Controller(s) version 7.11 or later.

You can configure an alert policy with an HTTP callback or an HTTP POST using PowerShell cmdlets. They are extended to support webhooks.

For information on the creation of a new Octoblu workflow and obtaining the corresponding webhook URL, see the Octoblu Developer Hub.

To configure a webhook URL for a new alert policy or for an existing policy, use the following PowerShell cmdlets.

Create alerts policy with a webhook URL:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

Add a webhook URL to an existing alerts policy:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

For help on the **PowerShell** commands, use the PowerShell help, for example:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

Notifications generated from the alert policy trigger the webhook with a POST call to the webhook URL. The POST message contains the notification information in JSON format:

```
{"NotificationId" : \<Notification Id\>,

"Target" : \<Notification Target Id\>,

"Condition" : \<Condition that was violated\>,

"Value" : \<Threshold value for the Condition\>,

"Timestamp": \<Time in UTC when notification was generated\>,

"PolicyName": \<Name of the Alert policy\>,

"Description": \<Description of the Alert policy\>,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or
dismissed\>,

"Site" : \<Site name\>}
```

Configure alerts policies with ServiceNow

You can configure alert policies to send notifications directly to ServiceNow (SNOW), enabling seamless integration with your IT Service Management (ITSM) workflows. This integration allows alerts generated in Citrix Monitor to be automatically forwarded to ServiceNow for centralized tracking, escalation, and incident resolution.

BENEFITS OF SERVICENOW INTEGRATION

- **Unified alert management**: Create, update, and manage ServiceNow incidents directly within the Citrix Monitor interface without switching between systems.
- **Automatic ITSM configuration**: Monitor automatically retrieves the required ServiceNow configuration, such as webhook URLs, reducing manual setup complexity.
- **Streamlined incident response**: Alerts are forwarded to ServiceNow for centralized incident tracking and resolution, improving operational efficiency.

PREREQUISITES

Before configuring ServiceNow integration, ensure the following:

- A ServiceNow instance is configured in the ITSM Adapter service.
- You have the necessary permissions to manage alert policies in Monitor.

CHECK SERVICENOW INTEGRATION STATUS

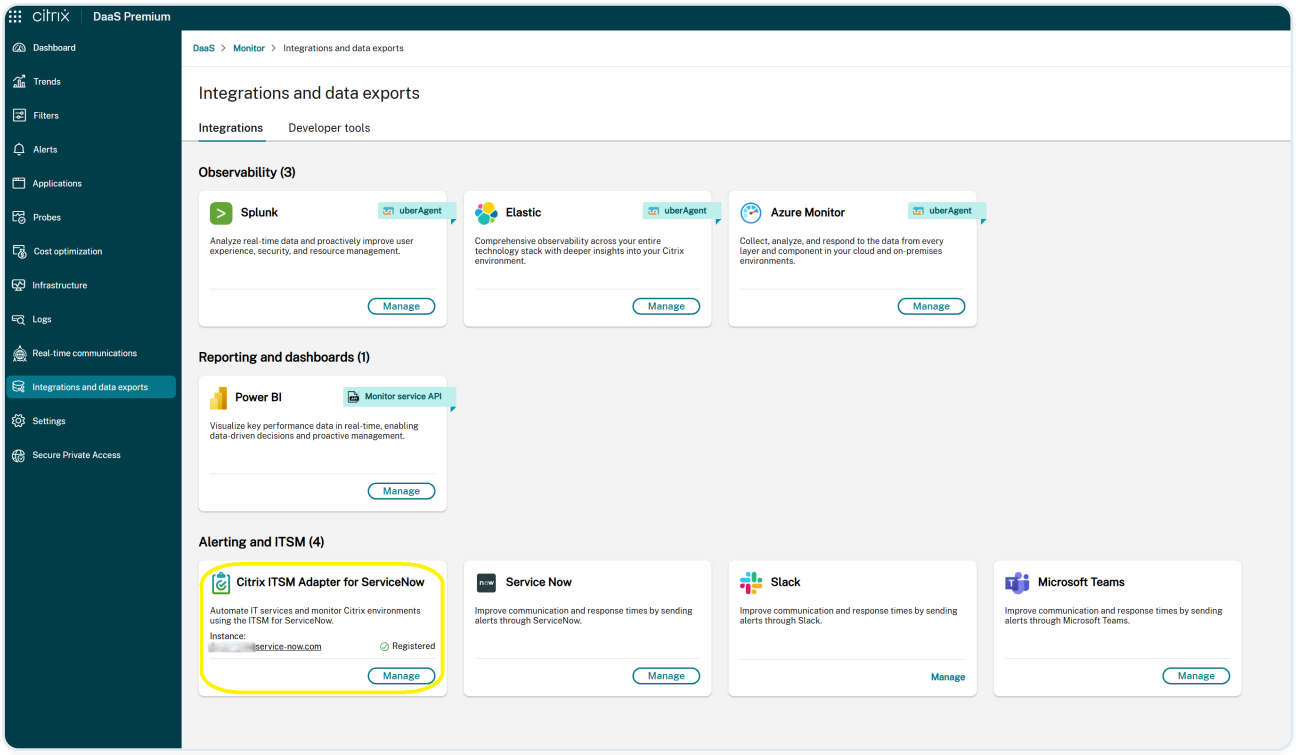
You can view the integration status with the ITSM Adapter service on the **Monitor** > **Integrations and Data Exports** page. This page displays:

- The current integration status:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Get Started**: Indicates that the ITSM Adapter integration has not been configured. Select this option to begin the initial setup process.
- **Manage**: Indicates that the ITSM Adapter integration is active and operational. Select this option to view or modify your ServiceNow integration settings.

- The associated ServiceNow instance URL (visible only when a ServiceNow instance has been configured in the ITSM Adapter).

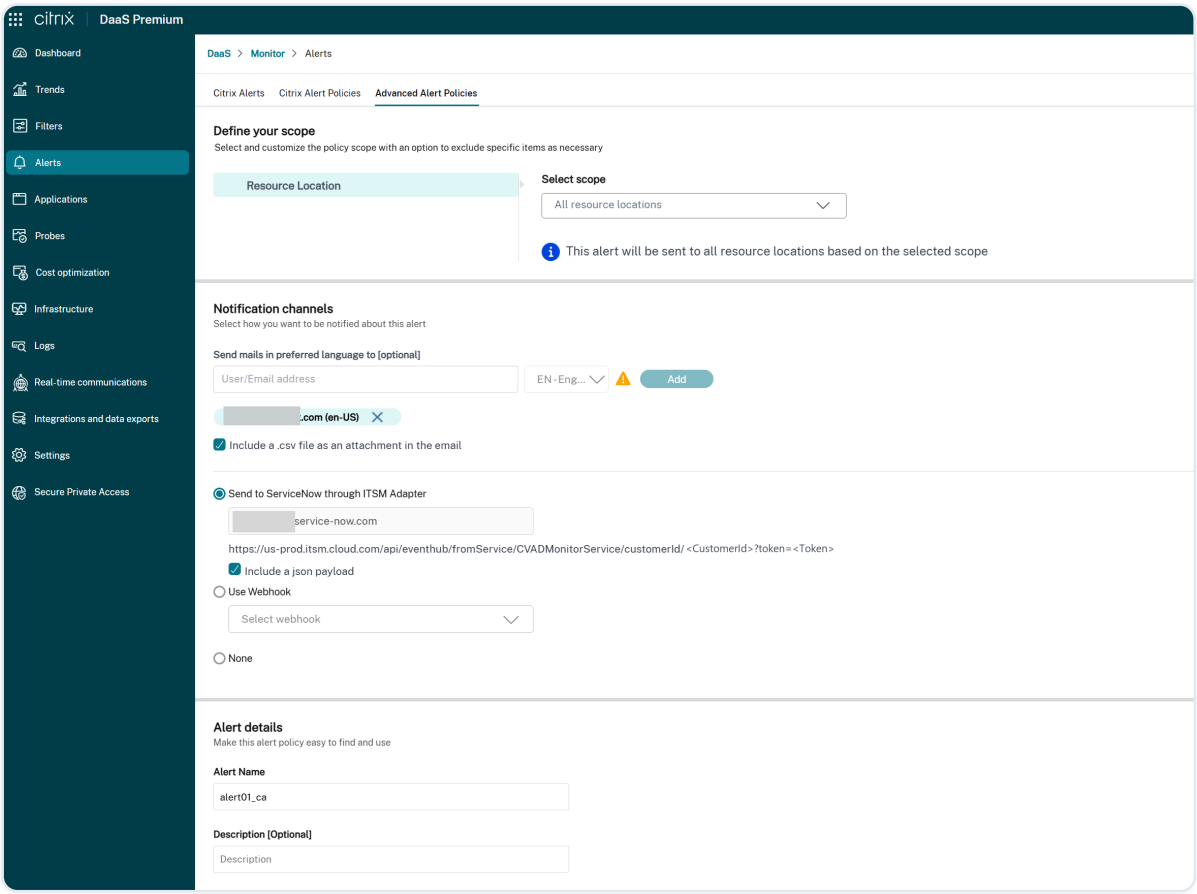


CONFIGURE AN ALERT POLICY WITH SERVICENOW NOTIFICATIONS

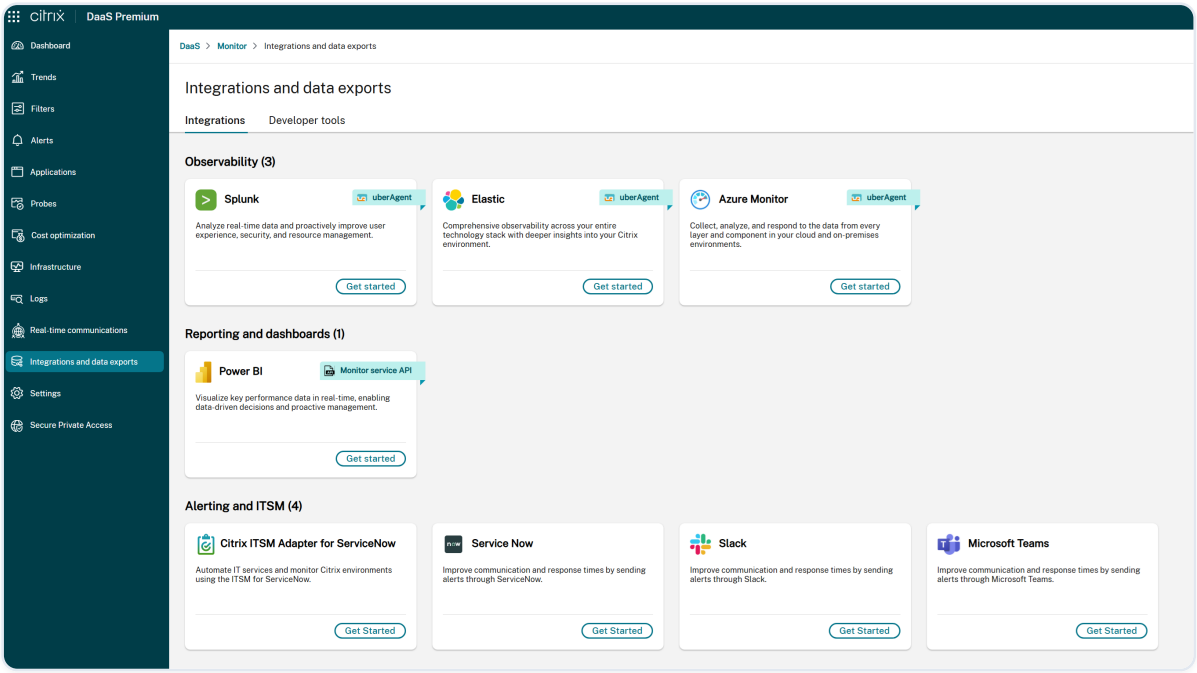
To configure an alert policy to send notifications to ServiceNow:

1. Go to **Alerts** > **Citrix Alerts Policy** and select the policy category (for example, Multi-session OS Policy).
2. Click **Create** to create a new policy or select an existing policy and click **Edit**.
3. Configure the policy conditions as required.
4. In the **Notification preferences** section, look for the **ServiceNow Integration** option:
   - **If the ITSM Adapter is available:**
     - Select the checkbox to enable alert notifications via ServiceNow for this policy.
     - The associated ServiceNow instance URL is displayed for reference.
     - If the policy already has a webhook configured, a warning message informs you that enabling ServiceNow integration overrides the existing webhook configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **If the ITSM Adapter is not available:**
  - A message indicates that ITSM integration is not currently configured.
  - Click **Get Started** to access integration setup. For details, refer to the documentation.



5. Click **Save** to save the policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Once configured, alerts that meet the policy conditions are automatically forwarded to ServiceNow, where they can be managed as incidents or events based on your ITSM configuration.

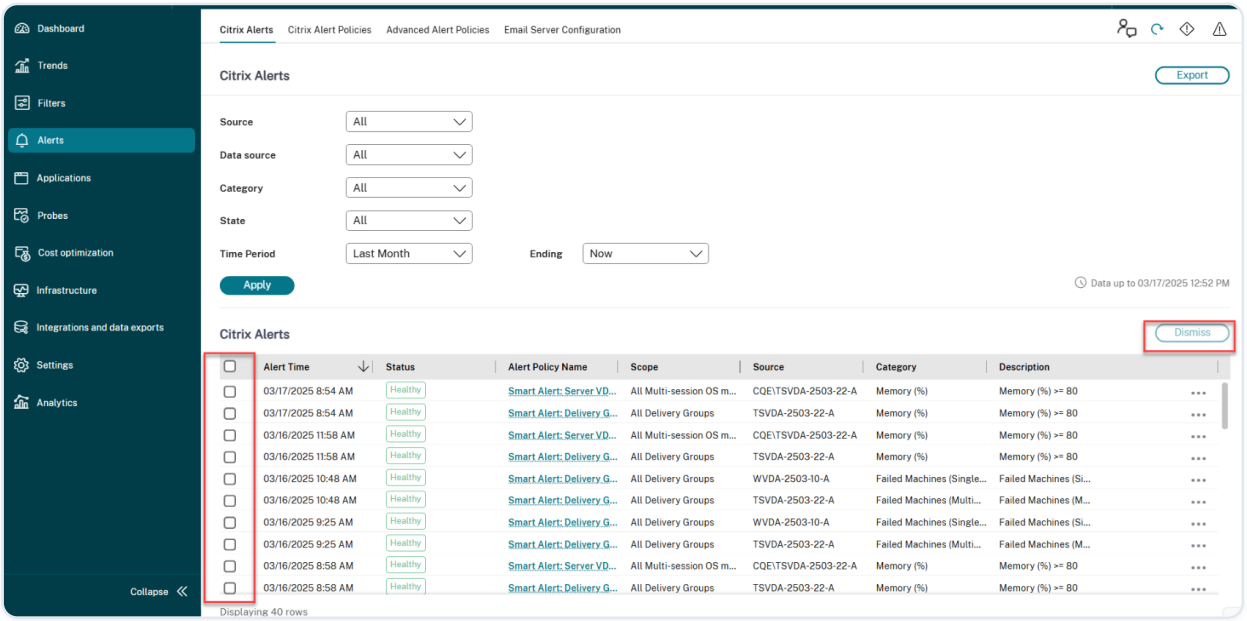
Bulk alert dismissal

This feature optimizes the alert management process for administrators, providing flexibility and reducing alert fatigue. Administrators can bulk dismiss alerts based on time, type, or category, simplifying alert management during maintenance or when dealing with hypervisors and other environments.

Bulk dismissal of alerts helps administrators manage their workload efficiently and prevents them from being overwhelmed by a high volume of alerts.

Steps to bulk dismiss alerts

1. Navigate to the **Alerts** > **Citrix Alerts** tab. The alerts are displayed.



2. Select an option from the **Source**, **Category**, **State**, or **Time Period** to filter the alerts that you want to dismiss. The specific alerts are displayed.
3. Select the checkbox next to a specific alert or at the top to select all alerts.
4. Click **Dismiss**. A notification appears to confirm the dismissal of alerts.
5. Click **Yes**. The selected alerts are marked as *dismissed*, and the status of the alert is updated accordingly.

Webhook configuration using PowerShell SDK

The webhook configuration feature using PowerShell SDK allows administrators to create, modify, delete, and list webhook profiles. This feature provides flexibility in configuring webhooks by

© 1997–2026 Citrix Systems, Inc. All rights reserved.

allowing the specification of headers, authentication types, content types, payloads, and webhook URLs.

NOTE:

The supported payload format is text and the end user must enable text in their webhook.

The latest payload format is:

```
{"text": "This is a message from a Webex incoming webhook."}
```

Create a webhook

You can use the following sample PowerShell command to create a webhook profile:

Create a webhook without authorization header:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"


Add-MonitorWebhookProfile -Name "webhookprofile1" -Description
"Description" -Url $url -Headers $headers -PayloadFormat $payloads
-Platform Slack -Type Webhook -MethodType POST
```

Create a webhook with authorization header:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")

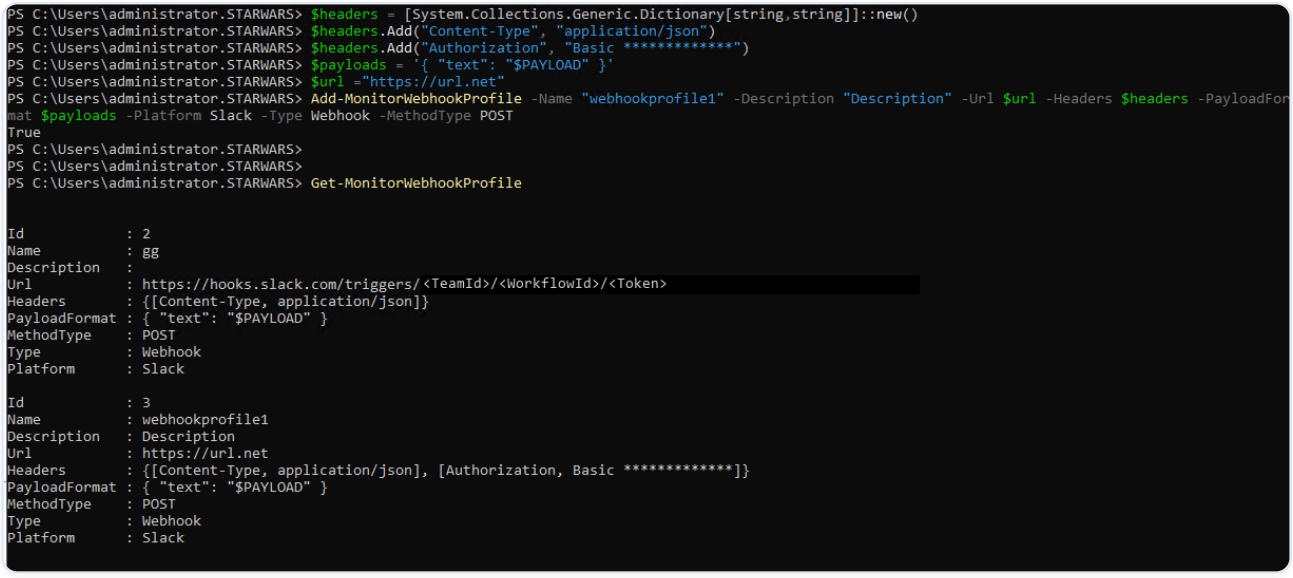

$headers.Add("Authorization", "Basic <Fill this field with the
authorization token>")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"

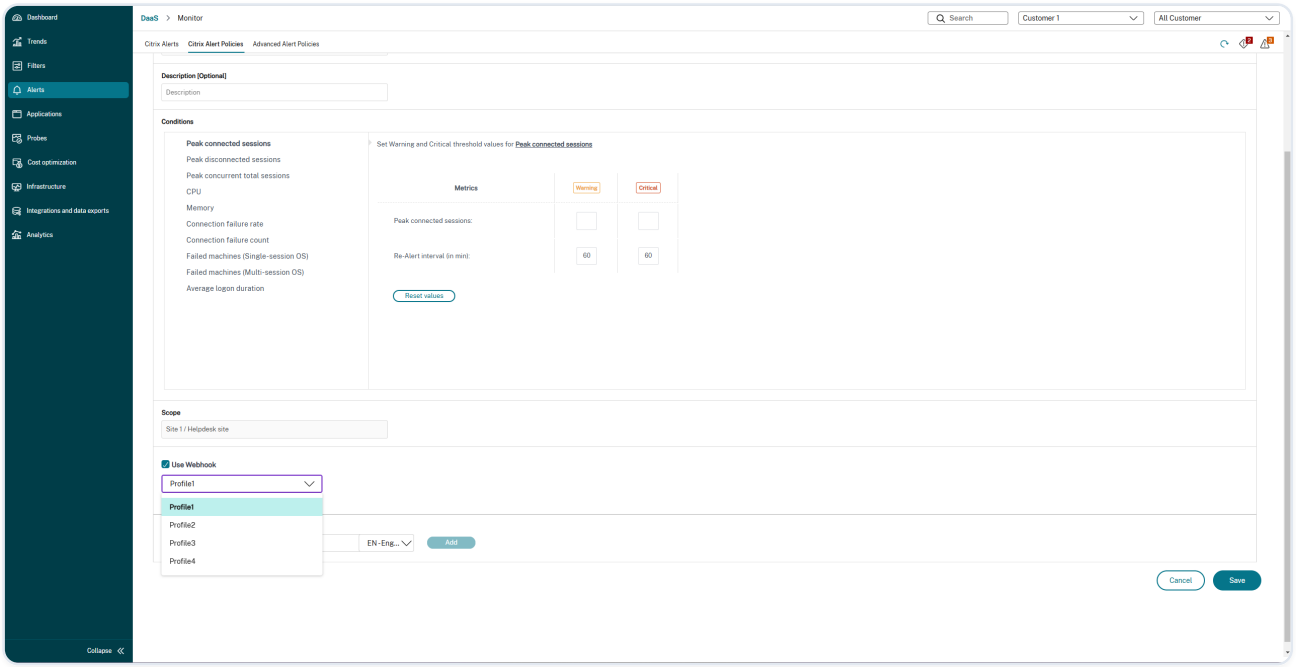

Add-MonitorWebhookProfile -Name "webhookprofile1" -Description
"Description" -Url $url -Headers $headers -PayloadFormat $payloads
-Platform Slack -Type Webhook -MethodType POST
```

Example:



Once the profile is created, you can check it in the database. Also, you can find the newly created webhook profile in the **Citrix Alerts** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Update a webhook profile

You can use the following sample PowerShell command to update a webhook profile:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")

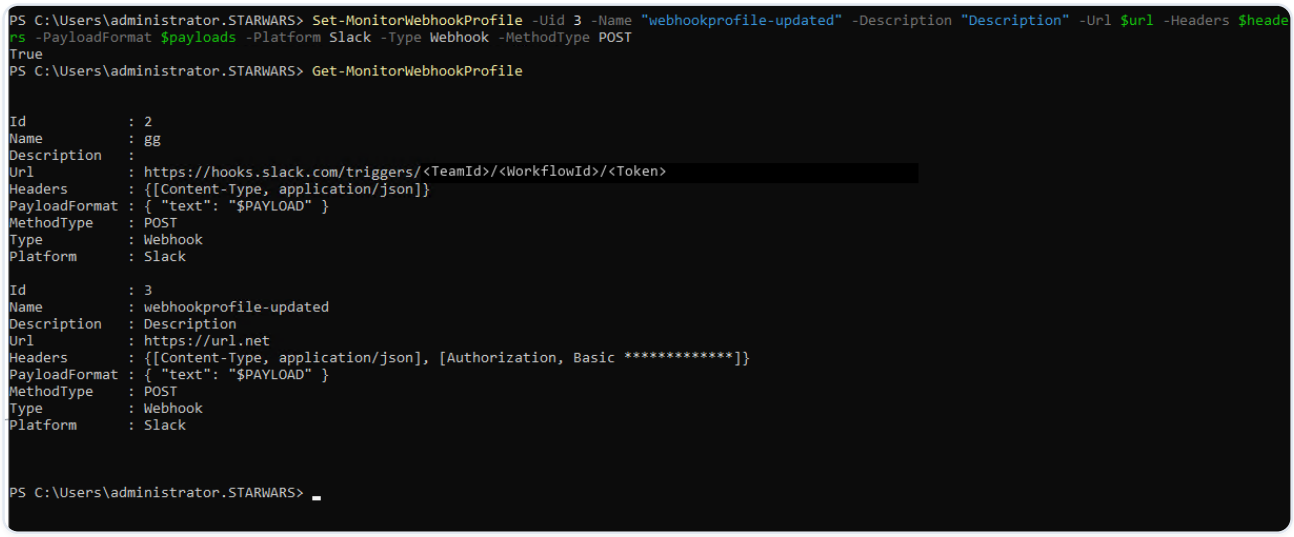

$payloads = '{ "text": "$PAYLOAD" }'


$url =  "<Fill this field with the required URL>"


Set-MonitorWebhookProfile -Uid 1  -Name "profile_slack_citrix"
-Description "webhook profile for citrix slack" -Url $url -Headers
$headers -PayloadFormat $payloads -Platform Slack -Type Webhook
-MethodType POST
```

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Get a list of all webhook profiles

You can use the following sample PowerShell command to get a list of all available webhook profiles:

```
Get-MonitorWebhookProfile



Get-MonitorWebhookProfile -Name 'profile_msteams'



Get-MonitorWebhookProfile -Uid 1
```

Remove a webhook profile

You can use the following sample PowerShell command to remove a webhook profile:

```
Remove-MonitorWebhookProfile -Uid 1
```

NOTE:

If a webhook profile is mapped to any policy, it cannot be removed. As a workaround, you must first remove the webhook mapping from the policy.

Create a policy with webhook profile

You can use the following sample PowerShell command to create a policy with webhook profile:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-MonitorNotificationPolicy -Name "Policy1" -Description "Policy
Description" -Enabled $true -WebhookProfileId 1
```

Update a policy with webhook profile

You can use the following sample PowerShell command to update a policy with webhook profile:

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 1
```

Remove webhook mapping from a policy

You can use the following sample PowerShell command to remove webhook profile from a policy:

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 0
```

Test webhook profile

You can use the following sample PowerShell command to test the webhook profile:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$headers.Add("Authorization", "Basic <Fill this with authorization
token>")


$payloads = '{ "text": "$PAYLOAD" }'


$url ="<Fill this field with the required URL>"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Test-MonitorWebhookProfile -Url $url -Headers $headers -PayloadFormat
$payloads
```

Local Host Cache config sync failure alert monitoring

Local Host Cache allows user sessions to continue even if Cloud Connectors lose connectivity with Citrix Cloud. The cache used by Local Host Cache is regularly synchronized with the primary database to ensure up-to-date configurations when Local Host Cache mode is activated. You can learn more information about Local Host Cache and the config sync process at Local Host Cache. If the configuration sync fails more than three times consecutively, Citrix Monitor sends a warning alert to the administrator.

A predefined alert policy named **Local Host Cache - Config Sync Failure** has been introduced in Citrix Monitor to notify administrators about configuration sync failures. You can find the newly introduced policy on **Monitor** > **Citrix Alerts**. You can modify the predefined policy to add or edit email recipients or webhooks to receive proactive notifications in your alert management or ITSM tools.

The scope of the **Local Host Cache - Config Sync Failure** alert policy is limited to the Site only.

Hypervisor Alerts Monitoring

Monitor displays alerts to monitor hypervisor health. Alerts from Citrix Hypervisor™ and VMware vSphere help monitor hypervisor parameters and states. The connection status to the hypervisor is also monitored to provide an alert if the cluster or pool of hosts is rebooted or unavailable.

To receive hypervisor alerts, ensure that a hosting connection is created in the **Manage** tab. For more information, see Connections and resources. Only these connections are monitored for hypervisor alerts. The following table describes the various parameters and states of Hypervisor alerts.

ALERT	SUPPORTED HYPERVISORS	TRIGGERED BY	CONDITION	CONFIGURATION
CPU usage	Citrix Hypervisor, VMware vSphere	Hypervisor	CPU usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.
Memory usage	Citrix Hypervisor,	Hypervisor	Memory usage alert threshold	Alert thresholds must be

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ALERT	SUPPORTED HYPERVISORS	TRIGGERED BY	CONDITION	CONFIGURATION
	VMware vSphere		is reached or exceeded	configured in the Hypervisor.
Network usage	Citrix Hypervisor, VMware vSphere	Hypervisor	Network usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.
Disk usage	VMware vSphere	Hypervisor	Disk usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.
Host connection or power state	VMware vSphere	Hypervisor	Hypervisor Host has been rebooted or is unavailable	Alerts are prebuilt in VMware vSphere. No additional configurations are needed.
Hypervisor connection unavailable	Citrix Hypervisor, VMware vSphere	Delivery Controller	Connection to the hypervisor (pool or cluster) is lost or powered down or rebooted. This alert is generated every hour as long as the connection is unavailable.	Alerts are prebuilt with the Delivery Controller. No additional configurations are needed.

NOTE:

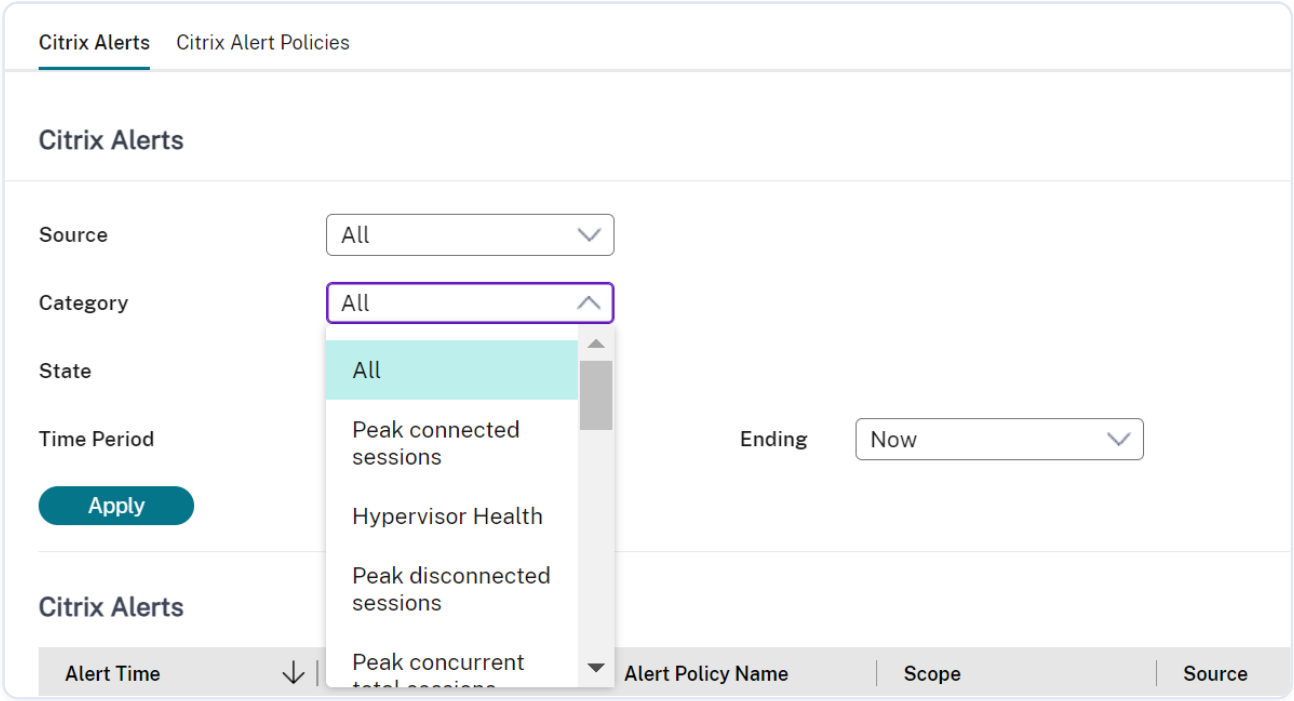
For more information about configuring alerts, see Citrix XenCenter Alerts or check the VMware vCenter Alerts documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Email notification preference can be configured under **Citrix Alerts Policy > Site Policy > Hypervisor Health**. The threshold conditions for Hypervisor alert policies can be configured, edited, disabled, or deleted from the hypervisor only and not from Monitor. However, modifying email preferences and dismissing an alert can be done in Monitor.

IMPORTANT:

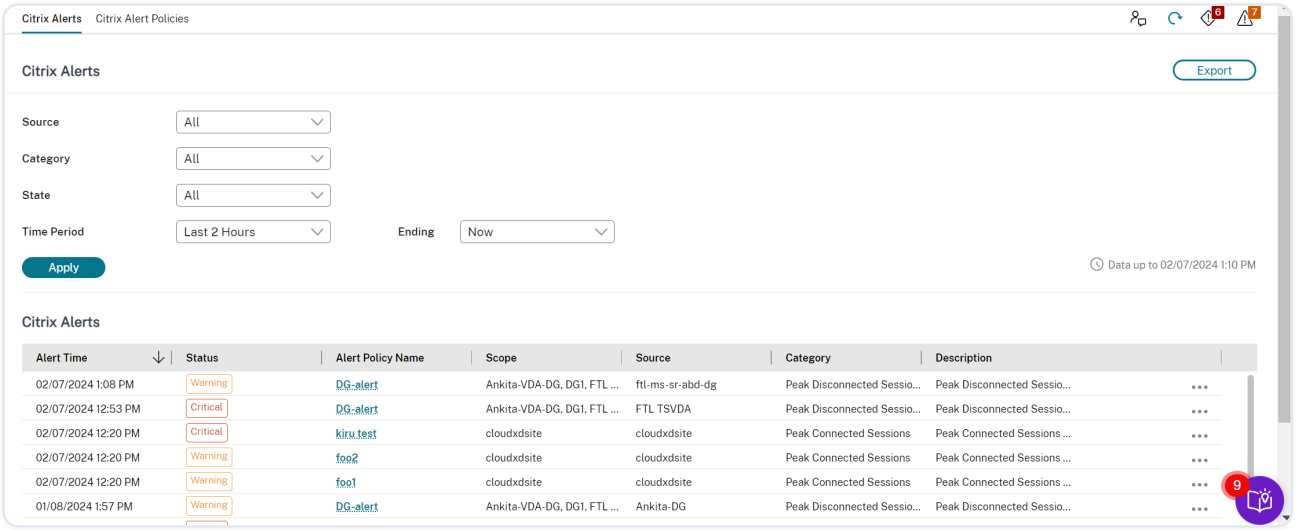
- All hypervisor alerts older than a day are automatically dismissed.
- Alerts triggered by the Hypervisor are fetched and displayed in Monitor. However, changes in the life cycle/state of the Hypervisor alerts are not reflected in Monitor.
- Alerts that are healthy or dismissed or disabled in the Hypervisor console will continue to appear in Monitor and have to be dismissed explicitly.
- Alerts that are dismissed in Monitor are not dismissed automatically in the Hypervisor console.



A new Alert category called **Hypervisor Health** has been added to enable filtering only the hypervisor alerts. These alerts are displayed once the thresholds are reached or exceeded. Hypervisor alerts can be:

- Critical—critical threshold of the hypervisor alarm policy reached or exceeded
- Warning—warning threshold of the hypervisor alarm policy reached or exceeded
- Dismissed—alert no longer displayed as an active alert

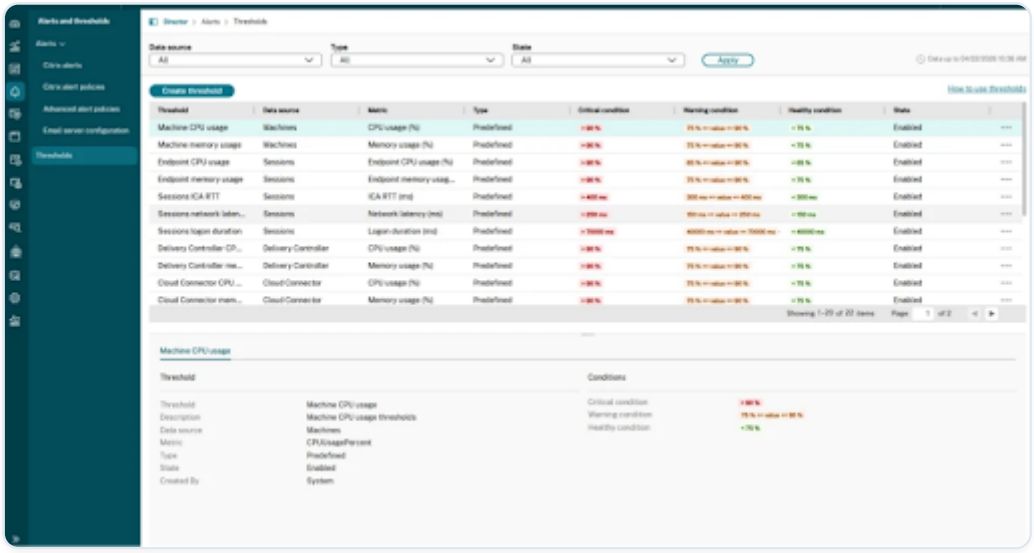
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Thresholds

Thresholds define visual health indicators for system metrics across the monitoring console. By setting Critical, Warning, and Healthy values for each metric, administrators can identify performance bottlenecks through color-coded indicators on multiple dashboard views.

Each threshold applies to a specific data source and metric combination. The system includes predefined thresholds based on Citrix best practices and supports custom thresholds that can be tailored to environment expectations. Enabled thresholds apply color-coded indicators to metric values across the console using Critical, Warning and Healthy values set by the administrator.

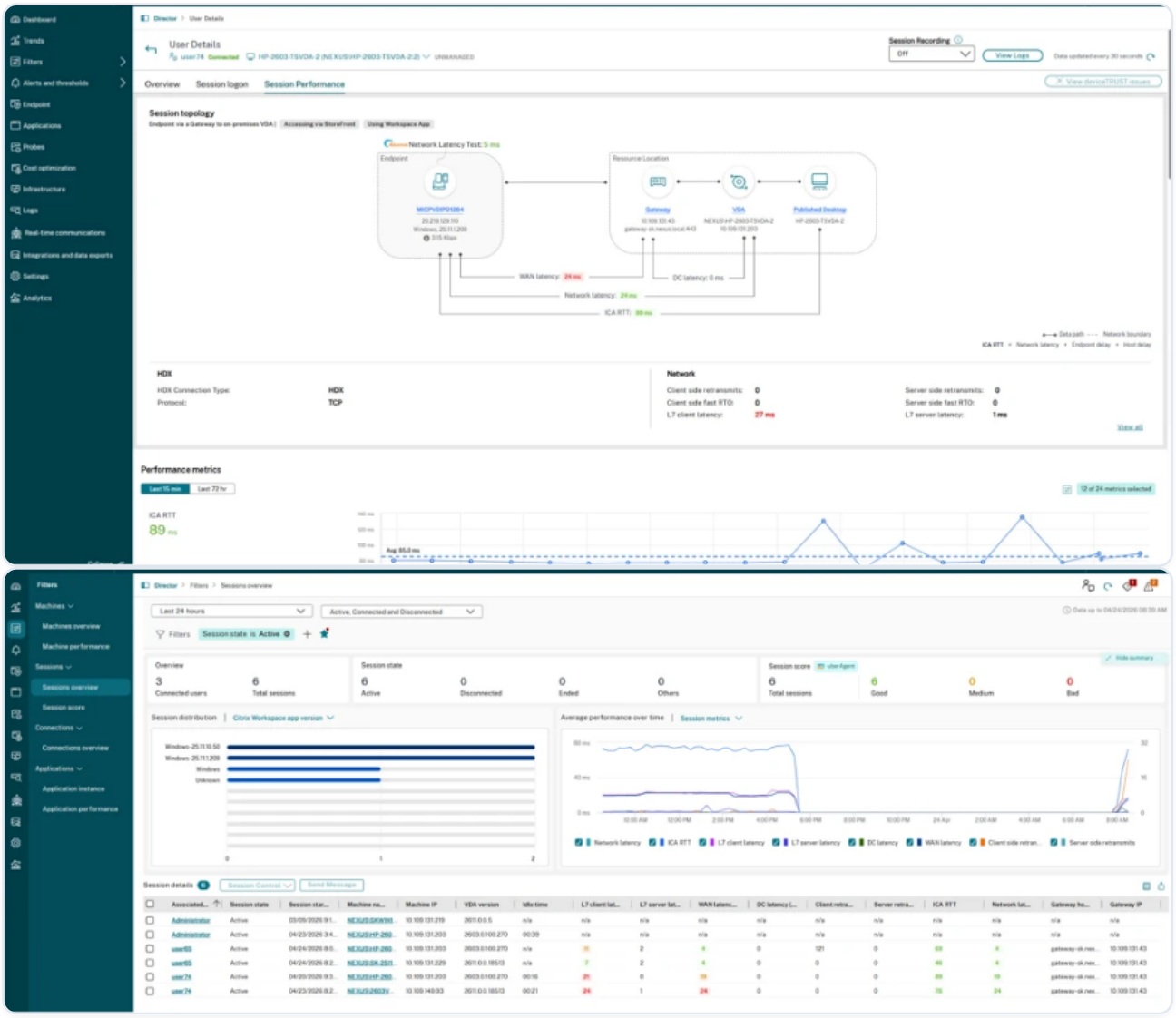


Thresholds update indicators on the following pages:

- **Dashboard** — Logon duration
- **Infrastructure** — Status for Delivery Controllers, Cloud Connectors, Provisioning Services, and StoreFront
- **Filters** — Performance metrics in Machines, Sessions, connections, and applications tables

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **User Details and Machine Details** — Per-user and per-machine metric indicators



Prerequisites

- Citrix DaaS™ 129 or Citrix Virtual Apps and Desktops™ 2611 or later
- Administrator permissions: Full administrator or authorized custom administrator

Predefined thresholds

Predefined thresholds are system-generated configurations based on Citrix best practices. These cannot be deleted but can be edited or disabled.

DATA SOURCE	METRIC	DEFAULT CRITICAL VALUE	DEFAULT WARNING VALUE	DYNAMIC
Machines	CPU usage %	90%	75%	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATA SOURCE	METRIC	DEFAULT CRITICAL VALUE	DEFAULT WARNING VALUE	DYNAMIC
Machines	Memory usage %	90%	75%	No
Sessions	CPU usage %	90%	75%	No
Sessions	Memory usage %	90%	75%	No
Sessions Endpoint	CPU usage %	90%	75%	No
Sessions Endpoint	Memory usage %	90%	75%	No
Sessions	ICA RTT	400 ms	300 ms	Yes (P90/P70)
Sessions	Network latency	250 ms	150 ms	Yes (P90/P70)
Sessions	Logon Duration	70,000 ms (70s)	40,000 ms (40s)	Yes (P90/P70)
Delivery Controller™	CPU usage %	90%	75%	No
Delivery Controller	Memory usage %	90%	75%	No
Cloud Connector	CPU usage %	90%	75%	No
Cloud Connector	Memory usage %	90%	75%	No
Provisioning service	CPU usage %	90%	75%	No
Provisioning service	Memory usage %	90%	75%	No
StoreFront™	CPU usage %	90%	75%	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATA SOURCE	METRIC	DEFAULT CRITICAL VALUE	DEFAULT WARNING VALUE	DYNAMIC
StoreFront	Memory usage %	90%	75%	No

To reset a predefined threshold to its factory defaults, select the threshold and choose **Use System Default**.

Custom thresholds

Custom thresholds are administrator-created configurations across the site. Unlike predefined thresholds, custom thresholds can be fully deleted.

Use custom thresholds to define metric boundaries for environments where the predefined defaults do not match operational expectations — for example, a tighter ICA RTT limit or utilization across VDAs.

Dynamic defaults

For ICA RTT, Network Latency, and Logon Duration, the system calculates default values every seven days based on the previous week's actual performance data.

- **Warning** — Set at the 70th percentile (P70): the value below which 70% of observations fall.
- **Critical** — Set at the 90th percentile (P90): the value below which 90% of observations fall.

Dynamic defaults allow thresholds to automatically adapt to the specific infrastructure baseline. Metrics are flagged only when they exceed levels typically experienced by the majority of the user base.

NOTE:

When **Use System Default** is selected for a dynamic metric, the system manages the threshold values automatically. Manually entered values override dynamic calculations until the threshold is reset.

Manage thresholds

Create a threshold

Navigate to **Thresholds** and select **Create Threshold**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STEP 1: SELECT DATA SOURCE AND METRIC

Select the data source (for example, Machines, Sessions) and the metric to monitor.

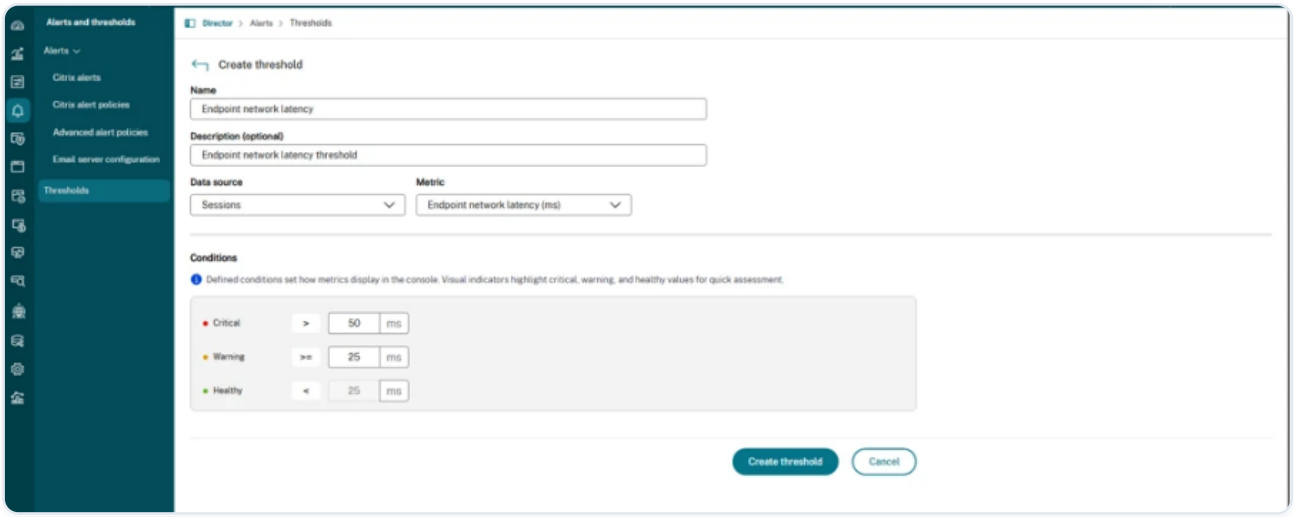
STEP 2: SET THRESHOLD VALUES

Enter values for the Critical and Warning states.

FIELD	DESCRIPTION
Critical value	The value above which the metric is flagged as Critical (red).
Warning value	The value above which the metric is flagged as Warning (amber).

STEP 3: SAVE

Select **Save** to activate the threshold. Color-coded indicators appear on applicable pages immediately.

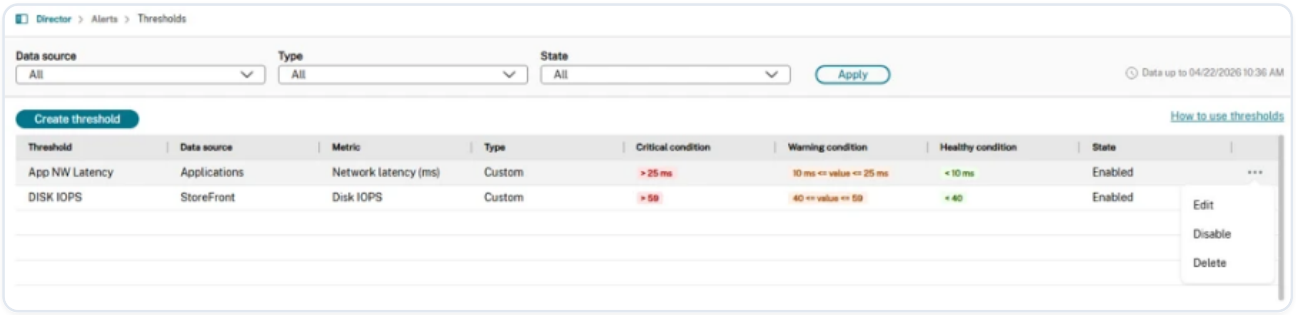


Edit a threshold

Select a threshold from the list and choose **Edit**. Modify the Critical or Warning values and select **Save**.

For predefined thresholds, select **Use System Default** to revert to Citrix-recommended values. For dynamic metrics, this re-enables automatic P70/P90 calculations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Disable a threshold

Select a threshold and choose **Disable**. Disabling a threshold reverts the metric to standard formatting on all pages without deleting the configuration. Re-enable the threshold at any time to restore color-coded indicators.

Delete a threshold

Select a custom threshold and choose **Delete**. Predefined thresholds cannot be deleted — disable them instead.

Troubleshooting

Dynamic default values appear unexpectedly high or low

Solution: Dynamic defaults reflect the P70 and P90 of the previous seven days of data. Unusual values indicate a period of abnormally high or low performance. If the calculated values do not match operational expectations, edit the threshold and enter manual values. Manual values override dynamic calculations. After one week of normal operations, reset the threshold to **Use System Default** to recalculate.

Predefined threshold values do not match the documented defaults

Solution: An administrator may have edited the predefined threshold. Select the threshold and choose **Use System Default** to restore factory defaults. For dynamic metrics (ICA RTT, Network Latency, Logon Duration), values are recalculated weekly. The current values reflect the most recent P70/P90 calculation, not the static defaults listed in the table above.

Application usage monitoring

Citrix Monitor helps you to monitor the usage of applications launched from the Citrix Workspace™ app session directly (also known as published applications)

The application usage reporting provides visibility into the most, least, and not used applications. The most used applications are presented on the Dashboard and contain curated charts. These

© 1997–2026 Citrix Systems, Inc. All rights reserved.

charts help the IT admins or application admins to gain insight into which applications are heavily used and the extent of their usage.

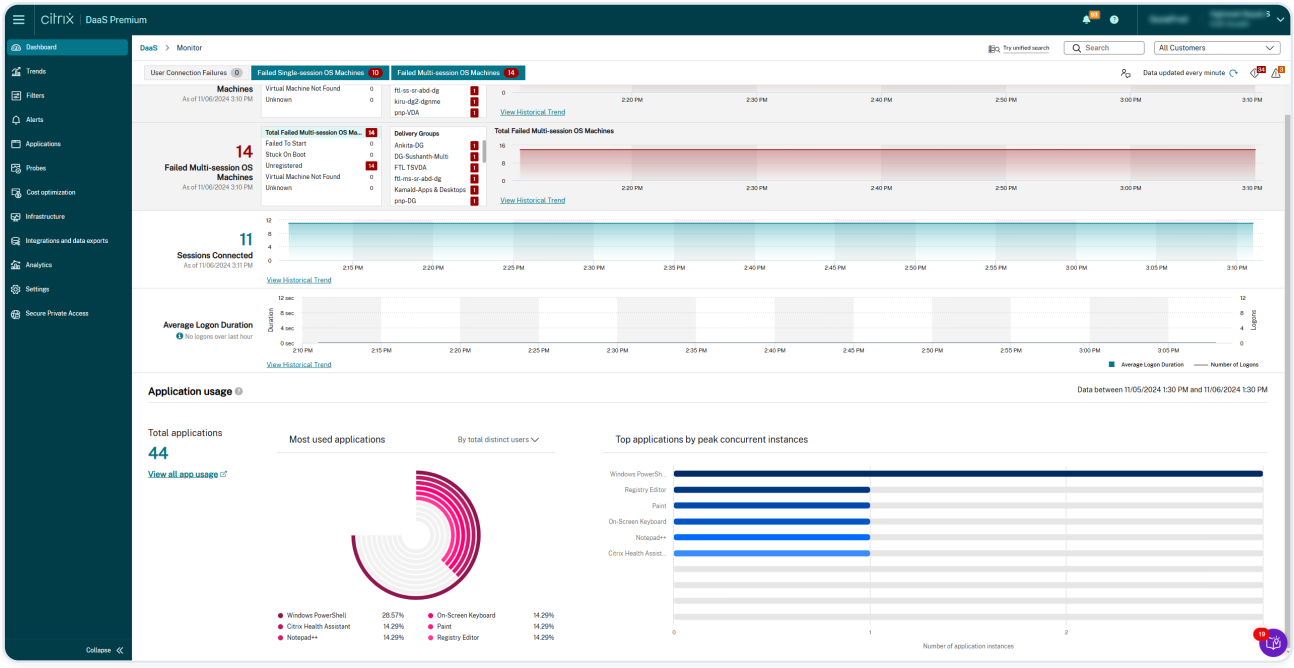
NOTE:

This feature is available only for the platinum-licensed sites.

With this feature, an admin can view which published applications are used the most. Using this data, admins can dive deeper into the extent of usage. Admin can analyze the details of the popular apps in the last 24 hours by the following data points:

- Total number of applications - Identifies the total number of applications in use by all the users in the enterprise's site.
- Most used applications by total number of distinct users - Identifies the top 10 apps by the total number of unique users.
- Most used applications by total number of application launches - Identifies the top 10 apps based on the total number of application launches.
- Top peak concurrent app instances - Identifies the top 10 apps based on the highest number of simultaneous instances of each application's usage. This information provides you the maximum demand for the applications listed.

This chart is present at the bottom of the Dashboard page. However, you can click **Check it out** on top of the screen to reach the chart directly.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also click **View all app usage** to view the details of a single app. This link opens the **Trends** > **Capacity Management** > **Hosted Application Usage** page.

The chart provides a visual representation of the app usage. Also, when you hover on the graph, you get the respective absolute counts of the selected data points. When you click any data point on the chart, the **Trends** > **Capacity Management** > **Hosted Application Usage** page opens with the specific app name selected. This data is to depict a comparative value against all the apps present in the enterprise's system. The absolute value of the data point is also mentioned separately in the same hover.

Least used and not used apps report

In a large Citrix DaaS™ environment, it's common to have many underutilized applications. To optimize your environment, the **Applications** page now offers extra metrics to help you understand application usage patterns within the organization and make data-driven decisions to improve resource allocation and cost savings.

Key features

- **Detailed usage information:** View distinct users (last 30 days), total launches, peak concurrent instances, and a trend chart of distinct users over time for each application.
- **Data focus:** Analyze application usage patterns over the last seven days, 30 days, or 90 days to assess application necessity. Viewing data for 90 days is recommended as it provides a quarter's worth of data, allowing you to observe whether application usage fluctuates or remains consistent. The dates on the X-axis help correlate organizational events with usage trends to determine if a drop was expected. This data empowers administrators to maintain efficient environments by eliminating unnecessary applications.
- **Optimization:** Identify total published apps, least used apps, and unused apps to optimize your Citrix deployment.
- **Actionable data:** Make data-driven decisions aiding application management to optimize resource allocation and license management.
- **Export data:** Export data in PDF or CSV format for further analysis. You can also export the data using Power BI integration or ODATA queries using application usage.

NOTE:

C>urrently, only published apps (referred to as desktop apps in the Citrix Workspace app) are included in this enhancement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements

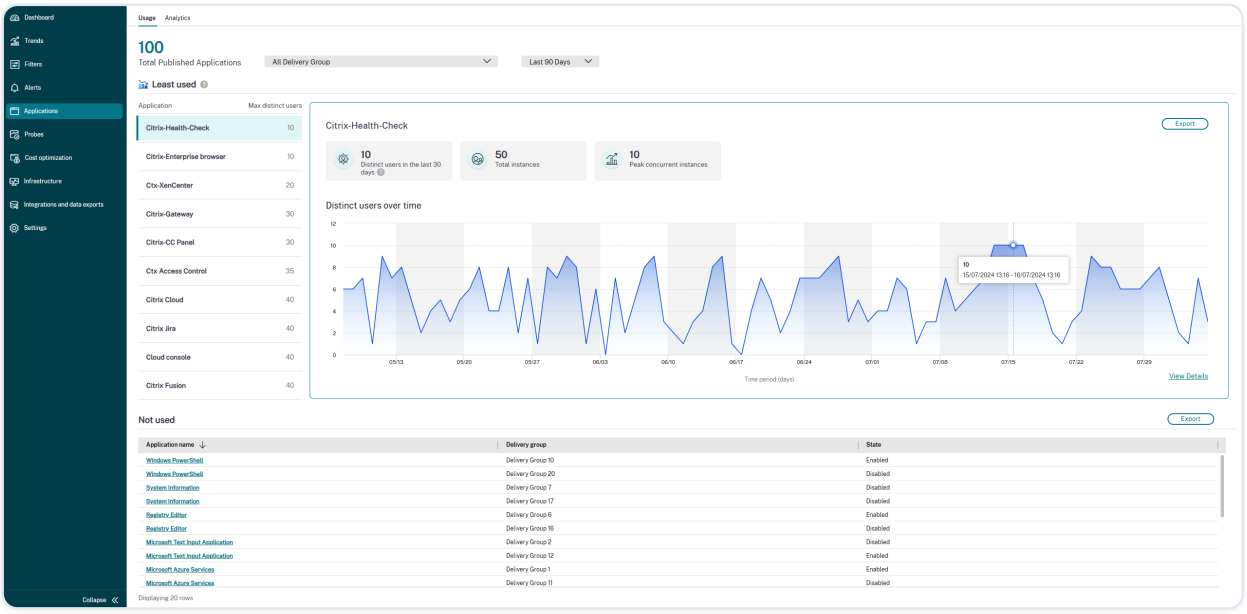
- VDAs version 7.15 or later

Viewing Application usage details

1. Click the **View apps** link in the **Review least used apps** section on the Dashboard.

   Or,

   Click the **Applications** tab. The following page appears:



2. Select the desired delivery group.
3. Select the required time period. (Note: For optimal analysis, the default is the last 90 days.)

   The following information is displayed:

   - **Total published applications:** Displays the total number of published applications.
   - **Least used:** Displays the apps with the fewest unique users over the selected time. The calculation is done as follows:

     a. **Daily user count:** The number of unique users for each app is counted daily.

     b. **Peak daily usage:** The highest daily user count for each app is identified.

     c. **Highest overall Usage:** The highest user count for each app across the selected timeframe is determined.

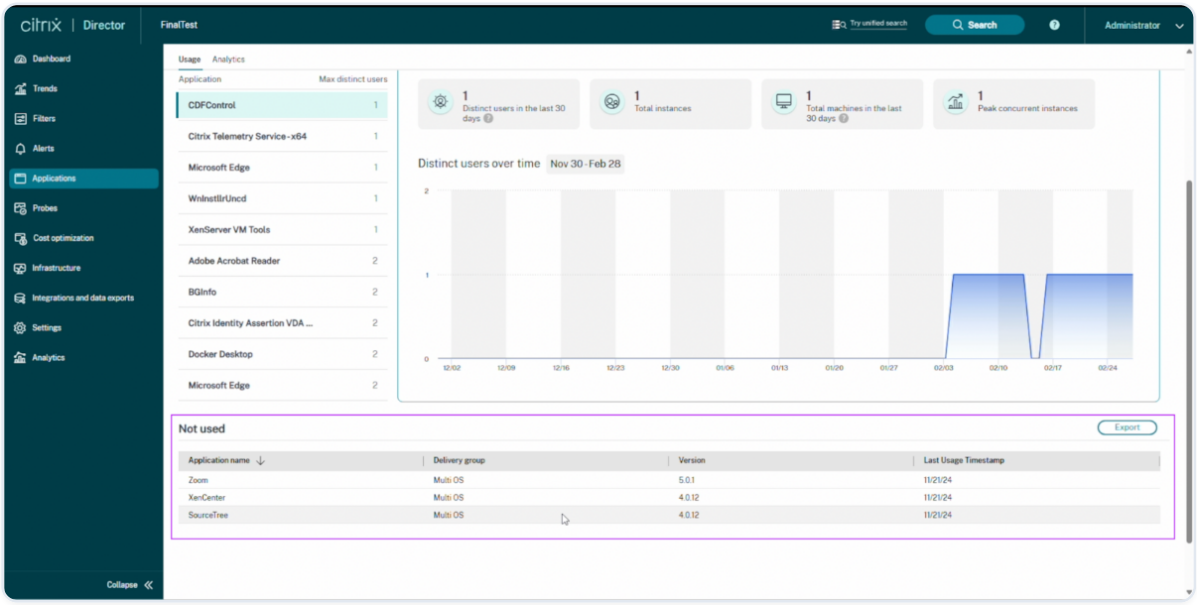
     d. **Ascending order:** The apps are listed in ascending order based on their highest overall user count, starting with the app with the lowest user count.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

It is recommended to select the last 90 days as the period for analysis. This range of days provides a quarter's worth of data and offers a comprehensive view of app usage patterns. However, options for filtering by seven days and one month are also available.

- **Not used:** Displays the applications that you have not been launched a single time in the last 90 days are listed. The delivery group that they were delivered through, the version of the app, and the exact timestamp of its last usage are provided. This information helps admins make informed decisions before removing an application from a virtual desktop.



4. Select an app from the **Least used** category to view detailed usage information, including:

   - **Distinct users in the last 30 days:** Displays the number of distinct users who accessed the app in the last 30 days. If you filter for seven days, this metric shows the distinct number of users for the selected app over those seven days.

NOTE:

Even when you select 90 days, this metric still displays data for the last 30 days only.

   - **Total launches:** Shows the number of times the app was launched.
   - **Peak concurrent instances:** Displays the highest number of instances running simultaneously.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Trend chart:** View a trend chart showing the number of distinct users over time for the selected app. Click **View details** to see more information in the **Capacity Management > Hosted Application Usage** section.

Usage of the trend chart

The trend chart illustrates the usage patterns, helping to identify trends and periods of low or high usage over the selected period. The X-axis represents the period in days, and the Y-axis represents the number of distinct users over time. By analyzing these metrics and the usage pattern graph, administrators can confidently optimize their Citrix DaaS environment.

You can use the trend chart in the following ways:

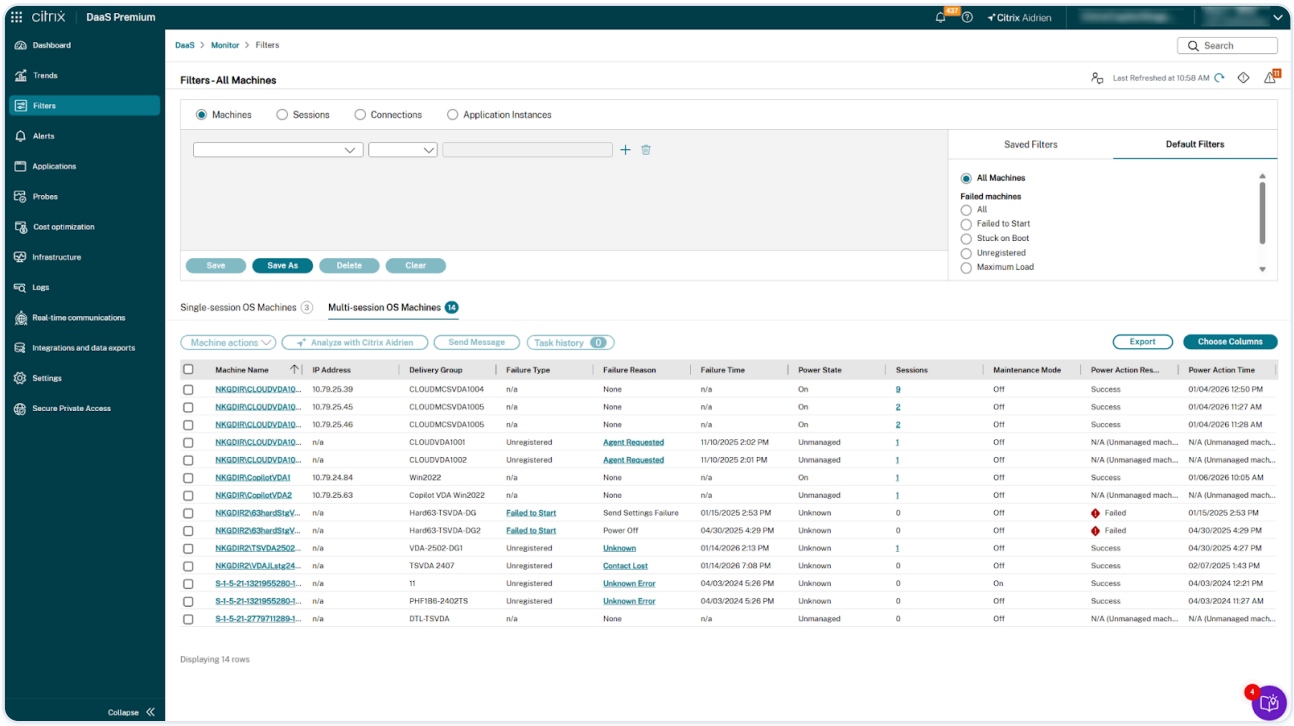
- **Hover over data points:** View the number of distinct users for the selected period.
- **View trends:** Identify usage patterns and determine whether app usage is consistent or just a temporary spike. This chart is useful for admins to monitor employee activity and identify potential issues or areas for improvement. For example, if an employee goes on vacation, there might be no application usage during that period. Once the employee returns, the application usage increases. The default filter for the period is 90 days that assists admins in making these calculations.
- **View details:** See the date and the corresponding number of distinct users.
- **Filter options:** Select different Time Period filter options to view the corresponding data.

Filter data to troubleshoot failures

When you click numbers on the Dashboard or select a predefined Default filter from the **Filters** tab, the Filters view opens to display data based on the selected machine or failure type.

You can create custom-filtered views of machines, connections, sessions, and application instances across all delivery groups and save the search for later access. You can edit a predefined filter and save it as a Saved filter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Select a view:

   - **Machines**. Select Single session OS Machines or Multi-session OS Machines. These views show the number of configured machines. The Multi-session OS Machines tab also includes the load evaluator index, which indicates the distribution of performance counters and tool tips of the session count if you hover over the link.
   - **Sessions**. You can also see the session count from the Sessions view. Use the idle time measurements to identify sessions that are idle beyond a threshold time period. Click the **Associated User** to open the Activity Manager for the user. Clicking the **Endpoint** name opens the Activity Manager for the Endpoint. Clicking **View Details** opens the **User Details** or **Endpoint Details** page respectively. For more information, see User Details.
   - **Connections**. Filter connections by different time periods, including last 60 minutes, last 24 hours, or last 7 days. Click the **Associated User** to open the Activity Manager for the user. Clicking the **Endpoint** name opens the Activity Manager for the Endpoint. Clicking **Machine Names** opens the Machine Details page. The **Machine Details** page lists the machine details, machine utilization, infrastructure details, and applied hotfixes. For more information, see Troubleshoot Machines.
   - **Application Instances**. This view displays the properties of all application instances on VDAs of Multi-session and Single session OS. The session idle time measurements are available for Application instances on VDAs of Multi-session OS.

2. Select a filter from the list of Saved or Default filters.
3. Use the drop-down lists to select further filter criteria.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select extra columns, as needed, to troubleshoot further.
5. Save and name your filter.
6. To open the filter later, from the Filters view, select View (Machines, Sessions, Connections, or Application Instances), and select the saved filter.
7. Click **Export** to export the data to CSV format files. Data of up to 100,000 records can be exported.
8. If needed, for **Machines** or **Connections** views, use machine actions for all the machines you select in the filtered list. For the Sessions view, use the session controls or option to send messages.

   NOTE:

   - Run Scripted Task is supported only when the WEM(Workspace Environment Management) service is provisioned and the WEM agent on the VDA is installed and registered with the WEM service.
   - Task History shows only the current user's Scripted Task executions within the last 24 hours.

9. If needed, you can use multiple actions. You get a progress bar on the progress of the action. Also, get a message when the action is complete.
10. In the **Machines** and **Connections** views, click the **Failure Reason** of a failed machine or connection to get a detailed description of the failure and actions recommended to troubleshoot the failure. The failure reasons and the recommended actions for Machine and Connection failures are available in the Citrix Director Failure Reasons Troubleshooting Guide.
11. In the **Machines** view, click a machine name link to go to the corresponding **Machine Details** page. This page displays the details of the machine, provides power controls, displays the CPU, memory, disk monitoring, and GPU monitoring graphs. Also, click **View Historical Utilization** to see the resource utilization trends for the machine. For more information, see Troubleshoot machines.
12. In the **Application Instances** view, sort or filter based on **Idle Time** greater than a threshold time period. Select the idle application instances to end. Log off or Disconnect of an application instance ends all active application instances in the same session. For more information, see Troubleshoot applications. The Application Instances filter page and idle time measurements in the Sessions filter pages are available if VDAs are version 7.13 or later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Studio allows assignment of multiple Desktop Assignment Rules (DAR) for different users or user groups to a single VDA in the delivery group. StoreFront displays the assigned desktop with the corresponding Display Name as per the DAR for the logged in user. However, Monitor does not support DARs and displays the assigned desktop using the delivery group name regardless of the logged in user. As a result, you cannot map a specific desktop to a machine in Monitor. To map the assigned desktop displayed in StoreFront to the delivery group name displayed in Monitor, use the following PowerShell command. Run the PowerShell command using Remote PowerShell SDK as described in the blog.

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

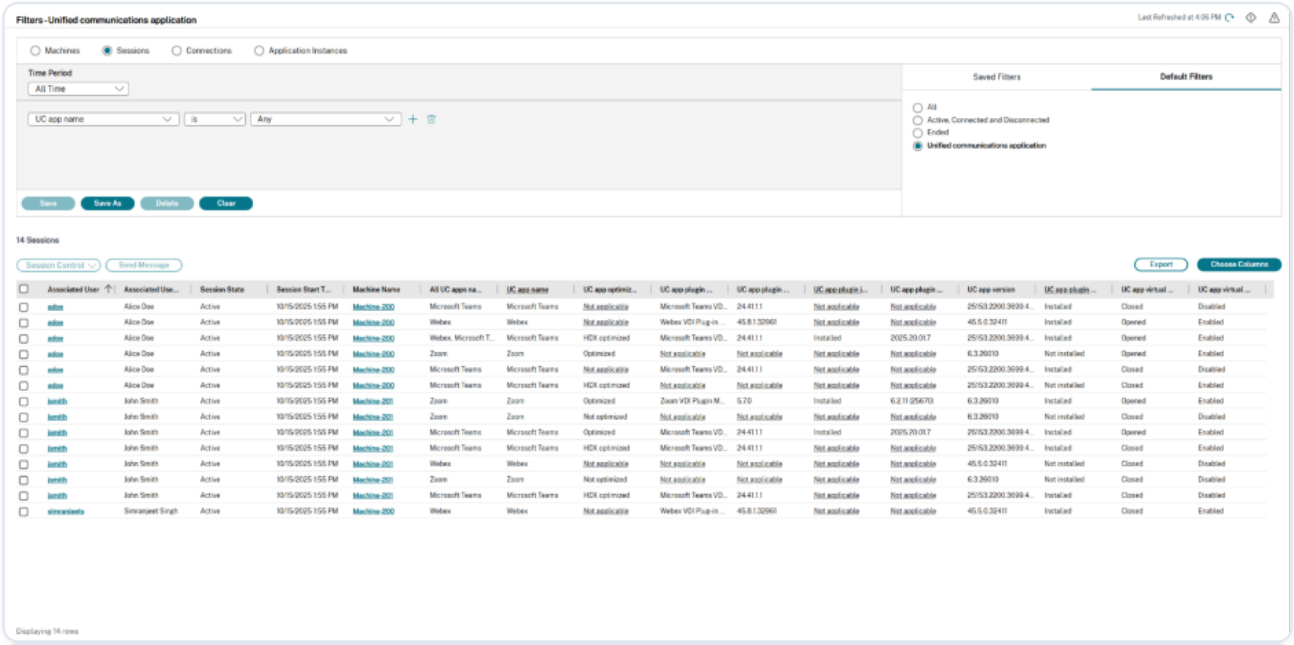
Unified Communication app metrics

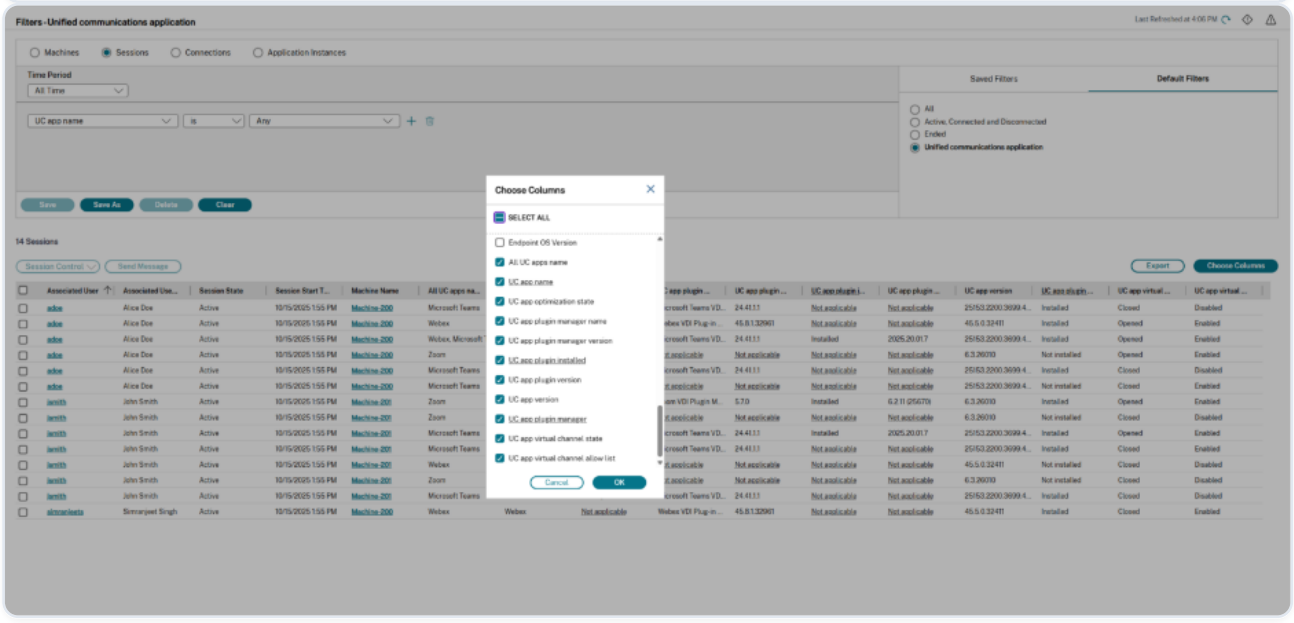
The **Sessions** view now includes several new display columns that provide detailed insights into Unified Communications (UC) application usage for a user session. These metrics are available in the filter to refine the list of sessions, and they can also be selected via the **Choose Columns** option to be displayed in the main session table view.

- **All UC apps name (Column Only)**: Contains data listing for all multiple UC applications that were running in the session simultaneously. This is a display column and not a filter option.
- **UC app name**: The name of the specific Unified Communications application (e.g., Microsoft Teams, Webex, Zoom).
- **UC app optimization state**: The optimization status of the UC application within the session (e.g., Optimized, HDX optimized, not optimized, not applicable).
- **UC app plugin manager name**: The name of the plugin manager used for the UC application.
- **UC app plugin manager version**: The version of the plugin manager being used.
- **UC app plugin installed**: Indicates whether the necessary application plugin is Installed or Not installed for the UC application.
- **UC app plugin version**: The version of the specific UC application plugin.
- **UC app version**: The overall version of the Unified Communications application.
- **UC app plugin manager**: Indicates whether the necessary application plugin manager is Installed or Not installed on the endpoint for the UC application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **UC app virtual channel state**: The status of the virtual channel established for the UC application (e.g., Opened, Closed).
- **UC app virtual channel allow list**: Indicates if the application's virtual channel is on the allowed list.





Monitor historical trends across a site

The Trends view accesses historical trend information of each site for the following parameters:

- sessions
- connection failures
- machine failures

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- logon performance
- load evaluation
- capacity management
- machine usage
- resource utilization

To locate this information, click the **Trends** menu.

The zoom-in drill down feature lets you navigate through trend charts by zooming in on a time period (clicking a data point in the graph) and drilling down to see the details associated with the trend. This feature enables you to better understand the details of who or what has been affected by the trends being displayed.

To change the default scope of each graph, apply a different filter to the data.

NOTE:

- Sessions, failures, and logon performance trend information are available as graphs and tables when the time period is set to Last month (**Ending now**) or shorter. When the time period is chosen as Last month with a custom ending date or as Last year, the trend information is available as graphs but not as tables.
- Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) supports historical data retention only for 90 days. Hence, one-year trends and reports in Monitor show the last 90 days of data.

Available trends

View trends for sessions: From the Sessions tab, select the delivery group and time period to view more detailed information about the concurrent session count.

The **Session Auto Reconnect** column displays the number of auto reconnects in a session. Auto reconnect is enabled when the Session Reliability or the Auto Client Reconnect policies are in effect. When there is a network interruption on the endpoint, the following policies come into effect:

- Session reliability comes into effect (by default for 3 minutes) where the Citrix Receiver™ or Citrix Workspace™ app tries to connect to the VDA.
- Auto client reconnect comes into effect between 3 and 5 minutes where the client tries to connect to the VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Both these reconnects are captured and displayed to the user. This information can take a maximum time of 5 minutes to appear on the Monitor UI after the reconnect occurs.

The auto reconnect information helps you view and troubleshoot network connections having interruptions, and to analyze networks having a seamless experience. You can view the number of reconnects for a specific delivery group or time period selected in the Filters.

A drilldown provides additional information like Session Reliability or Auto Client Reconnect, time stamps, Endpoint IP, and Endpoint Name of the machine where the Workspace app is installed.

By default, logs are sorted by the event time stamps in descending order. This feature is available for Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Receiver for Windows, and Citrix Receiver for Mac. This feature requires VDAs 1906 or later.

For more information about session reconnections, see Sessions. For more information about policies, see Auto client reconnect policy settings and Session reliability policy settings.

Sometimes, the auto reconnect data might not appear in Monitor for the following reasons:

- Workspace app is not sending auto reconnect data to VDA.
- VDA is not sending data to the Monitor service.

NOTE:

Sometimes, the client IP address might not be obtained correctly if certain Citrix Gateway policies are set.

View trends for connection failures: From the Failures tab, select the connection, machine type, failure type, delivery group, and time period to view a graph containing more detailed information about the user connection failures across your site.

View trends for machine failures: From the Single session OS Machine Failures tab or Multi-session OS Machines tab, select the failure type, delivery group, and time period to view a graph containing more detailed information about the machine failures across your site.

View trends for logon performance: From the Logon Performance tab, select the delivery group and time period to view a graph containing more detailed information about the duration of user logon times across your site and whether the number of logons affects the performance. This view also shows the average duration of the logon phases, such as brokering duration and VM start time. This data is specifically for user logons and does not include users trying to reconnect from disconnected sessions. The table below the graph shows Logon Duration by User Session. You

© 1997–2026 Citrix Systems, Inc. All rights reserved.

can choose the columns to display and sort the report by any of the columns. You can also export these reports to a .CSV file. For more information, see Diagnose user logon issues.

View trends for load evaluation: From the Load Evaluator Index tab, view a graph containing more detailed information about the load that is distributed among Multi-session OS machines. The filter options for this graph include the delivery group or Multi-session OS machine in a delivery group, Multi-session OS machine (available only if a Multi-session OS machine in a delivery group was selected), and range. The Load Evaluator Index is displayed as percentages of Total CPU, Memory, Disk or Sessions and is shown in comparison with the number of connected users in the last interval.

View trends for local host cache: From the **Local Host Cache tab**, select the time period, zone, and cloud connector to view the detailed information on data missed during the outage such as number of machines registered, number of machines reconnected, and number of sessions brokered within your site. The displayed data is based on the selected time period, zone, and cloud connector.

You can also view data for all zones and cloud connectors. The default-selected data is for the last 24 hours and for all zones and cloud connectors. The local host cache data is available for the last 2 hours, 24 hours, 7 days, month, and 90 days. The maximum data available is for the last 90 days. For more information on local host cache, see the Local Host Cache documentation. The view shows the following local host cache data per selected zone and cloud connector for the selected time period:

- Start time of the outage
- End time of the outage
- Duration of the outage
- New sessions brokered during the outage
- Number of sessions reconnected during the outage
- Number of machines registered during outage
- Number of machines affected during outage
- The name of the zone
- The name of the cloud connector

View hosted applications usage: From the Capacity Management tab, select the Hosted Applications Usage tab, select the delivery group and time period to view a graph displaying peak concurrent usage and a table displaying application based usage. From the Application Based

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Usage table, you can choose a specific application to see details and a list of users who are using, or have used, the application.

View single and multi-session OS usage: The Trends view shows the usage of Single session OS by site and by delivery group. When you select site, usage is shown per delivery group. When you select delivery group, usage is shown per User. The Trends view also shows the usage of Multi-session OS by site, by delivery group, and by Machine. When you select site, usage is shown per delivery group. When you select delivery group, usage is shown per Machine and per User. When Machine is selected usage is shown per User.

View virtual machine usage: From the **Machine Usage** tab, select **Single session OS Machines** or **Multi-session OS Machines** to obtain a real-time view of your VM usage. The page displays the number of Autoscale™ enabled Multi-session and Single session OS machines that are powered on for a selected delivery group and time period. Also available is the estimated savings achieved by enabling Autoscale in the selected delivery group. This percentage is calculated using the per machine costs.

The usage trends of Autoscale-enabled machines indicate the actual usage of the machines, enabling you to quickly assess your site's capacity needs.

- Single session OS availability - displays the current state of Single session OS machines (VDIs) by availability for the entire site or a specific delivery group.
- Multi-session OS availability - displays the current state of Multi-session OS machines by availability for the entire site or a specific delivery group.

You can click the following links on the banner displayed to gain better visibility into machine usage with Cost optimization:

- Estimated savings - This link directs you to the **Estimated savings** section on the **Cost optimization** page, displaying details of all delivery groups.
- Savings report - This link directs you to the **Savings report** section on the **Cost optimization** page, displaying details of all delivery groups.

NOTE:

The grid below the chart displays the delivery group-based machine usage data in real-time. The data includes machine availability of all machines independent of Autoscale enablement. The number of machines displayed in the Available Counter column in the grid includes machines in maintenance mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The monitoring data consolidation depends on the time period that you select.

- Monitoring data for the one day and one week time periods is consolidated per hour.
- Monitoring data for the one month time period is consolidated per day.

The machine status is read at the time of consolidation and any changes during the period in between is not considered. For the consolidation period, refer to the Monitor API documentation.

For more information on monitoring Autoscale enabled machines see the Autoscale article.

View resource utilization: From the **Resource Utilization** tab, select **Single session OS Machines or Multi-session OS Machines** to obtain insight into historical trends data for CPU and memory usage, and IOPS and disk latency for each VDI machine for better capacity planning. This feature requires VDAs **version 7.11** or later. The graphs show data for average CPU, average memory, average IOPS, disk latency, and peak concurrent sessions. You can drill down to the machine, and view data and charts for the top 10 CPU consuming processes. Filter by delivery group and Time period. CPU, memory usage, and peak concurrent sessions graphs are available for the last 2 hours, 24 hours, 7 days, month, and year. The average IOPS and disk latency graphs are available for the last 24 hours, month, and year.

You can click the **Check out link** on the banner to gain better visibility into machine usage with Cost optimization. This link takes you to the **Workload rightsizing** tab in the **Cost optimization** page, displaying details of the selected delivery group from the **Resource Utilization** tab.

NOTE:

- The Monitoring policy setting, Enable Process Monitoring, must be set to "Allowed" to collect and display data in the Top 10 Processes table on the Historic Machine Utilization page. The policy is set to "Prohibited" by default. All resource utilization data is collected by default. This can be disabled using the Enable Resource Monitoring policy setting. The table below the graphs shows the resource utilization data per machine.
- Average IOPS shows the daily averages. Peak IOPS is calculated as the highest of the IOPS averages for the selected time range. (An IOPS average is the hourly average of IOPS collected during the hour on the VDA).
- The machine drilldown lists processes with average CPU or average memory usage more than 1%, this might mean that sometimes fewer than 10 processes are listed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View application failures: The Application Failures tab displays failures associated with the published applications on the VDAs.

This feature requires VDAs **version 7.15** or later. Single session OS VDAs running Windows Vista and later, and Multi-session OS VDAs running Windows Server 2008 and later are supported. For more information, see Historical application failure monitoring.

By default, only application faults from Multi-session OS VDAs are displayed. You can set the monitoring of application failures by using Monitoring policies. For more information, see Monitoring policy settings.

Create customized reports: The Custom Reports tab provides a user interface for generating Custom Reports containing real-time and historical data from the Monitoring database in tabular format.

From the list of previously saved Custom Report queries, you can click **Run and download** to export the report in CSV format, click **Copy OData** to copy and share the corresponding OData query, or click **Edit** to edit the query. You can create a Custom Report query based on machines, connections, sessions, or application instances. Specify filter conditions based on fields such as machine, delivery group, or time period. Specify the extra columns required in your Custom Report. Preview displays a sample of the report data. Saving the Custom Report query adds it to the list of saved queries.

You can create a Custom Report query based on a copied OData query. To do this, select the OData Query option and paste the copied OData query. You can save the resultant query for execution later.

NOTE:

The column names in the Preview and Export report generated using OData queries are not localized, but appear in English.

The flag icons on the graph indicate significant events or actions for that specific time range. Hover the mouse over the flag and click to list events or actions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- HDX™ connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.
- Delivery groups deleted in Studio are available for selection in the Trends filters until data related to them are groomed out. Selecting a deleted delivery group displays graphs for available data until retention. However, the tables don't show data.
- Moving a machine containing active sessions from one delivery group to another causes the **Resource Utilization and Load Evaluator Index** tables of the new delivery group to display metrics consolidated from the old and new delivery groups.

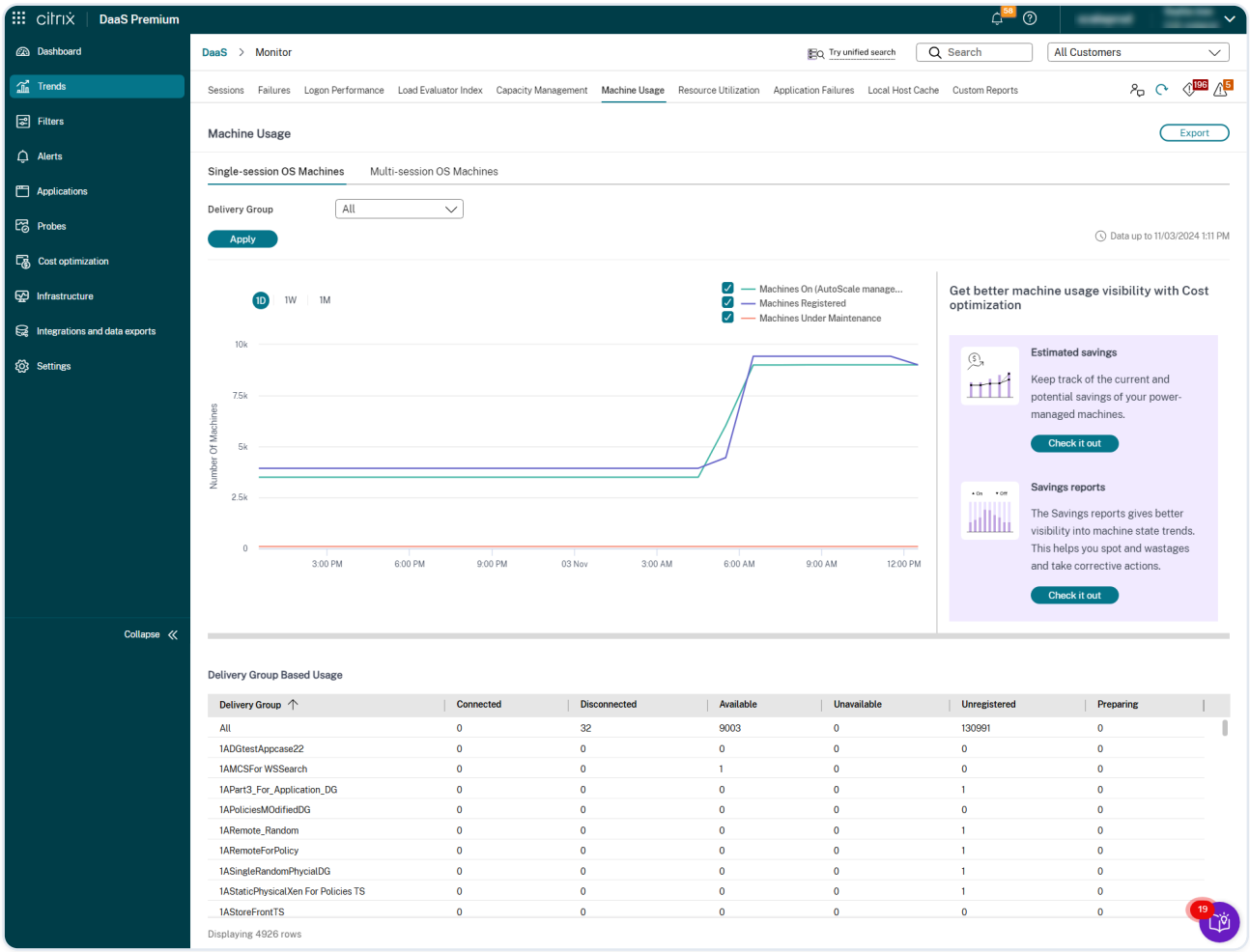
Monitor Autoscale-managed machines

Autoscale is a power management feature that enables proactive power management of all registered Multi-session and Single session OS machines in a delivery group. You can configure Autoscale for a selected delivery group from the **Manage** tab. For more information, see Autoscale. You can monitor the key metrics of Autoscale enabled machines from the **Monitor** console.

Machine Usage

The **Monitor** > **Trends** > **Machine Usage** page displays the total number of Autoscale enabled Multi-session and Single session OS machines that are powered on for a selected delivery group and time period. This metric indicates the actual usage of machines in the delivery group. From the **Single session OS Machines** or the **Multi-session OS Machines** tab, select the Delivery group and the time period.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



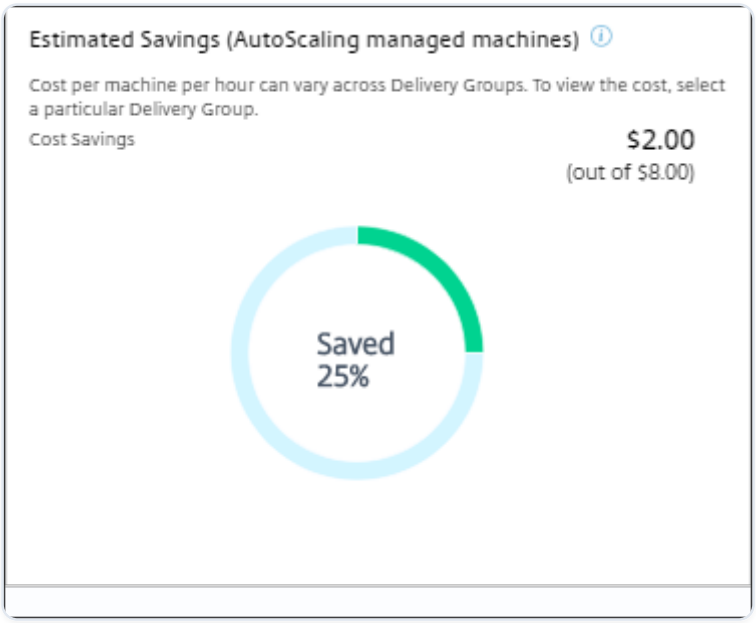
The chart plots the following metrics:

- **Machines On** - the number of Autoscale enabled machines that are powered on
- **Machines Registered** - the number of registered Multi-session or Single session OS machines
- **Machines under Maintenance** - the number of Multi-session or Single session OS machines with maintenance mode switched on

Estimated Savings

The **Monitor** > **Trends** > **Machine Usage** page also displays the estimated cost savings achieved by enabling Autoscale in the selected delivery group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Estimated Savings is calculated as the percentage of savings per machine per hour (in US $) as configured in **Manage** > **Edit Delivery Group** > **Autoscale**. For more information about configuring the savings per machine, see Autoscale.

When you select all Delivery groups, the average value of Estimated Savings across all the delivery groups is displayed. The estimated savings help administrators consolidate the existing infrastructure and plan the capacity to achieve maximum savings and utilization.

Alert notifications for machines and sessions

The Monitor Dashboard displays alert notifications that can be further drilled down. Alert details are displayed on the **Monitor** > **Alerts** page.

- To create an alert policy in a delivery group, go to **Monitor** > **Alerts** > **Citrix Alerts Policy** > **Delivery Group Policy**.
- Here, you can set the following Warning and Critical thresholds:
  - Failed Machines (Single session OS) and Failed Machines (Multi-session OS),
  - Peak Connected Sessions, Peak Disconnected Sessions and Peak Concurrent Total Sessions in the delivery group.
- Alerts are generated when the corresponding metric in the delivery group reaches the threshold.

For more details regarding the alert policy conditions and creation of new alert policies, see Alerts and notifications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Machine status

- **Monitor** > **Filters** > **Machines** displays the power state of all machines in a tabular format. You can filter by a specific delivery group.
- **Monitor** > **Filters** > **Sessions** displays filter by the Machine name to see the associated sessions and their real-time status.
- In **Monitor** > **Trends** > **Sessions**, select your delivery group and time period to see the trend of the sessions and their associated metrics.

For more information, see Filter data to troubleshoot failures.

Load Evaluation trends

The **Monitor** > **Trends** > **Load Evaluator Index** page displays a graph with detailed information about the load that is distributed among the Multi-session OS machines. The filter options for this graph include the delivery group or Multi-session OS machine in a delivery group, Multi-session OS machine (available only if Multi-session OS machine in a delivery group was selected), and range. The Load Evaluator Index is displayed as percentages of Total CPU, Memory, Disk, or Sessions and is shown in comparison with the number of connected users in the last interval.

Troubleshoot deployments

As a help desk administrator, you can search for the user reporting an issue. And, then display details of sessions or applications associated with that user.

Similarly, you can search for machines or endpoints where issues are reported. Issues can be quickly resolved by monitoring the relevant metrics and performing suitable actions.

The following actions are available:

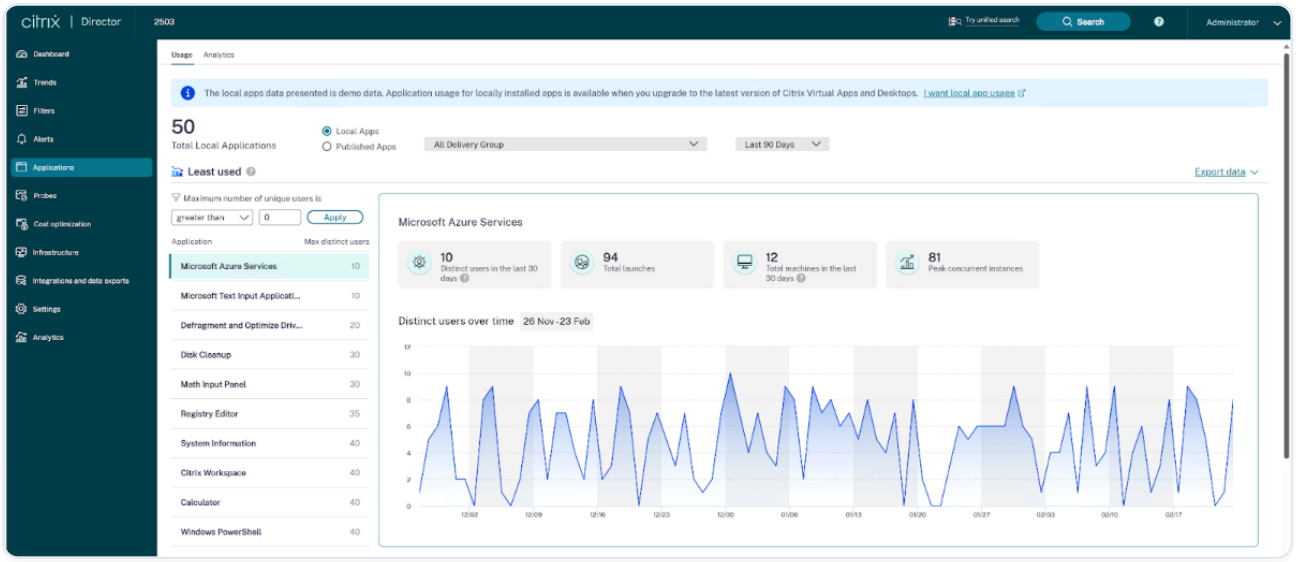
- ending an unresponsive application or process
- shadowing operations on the user's machine
- logging off an unresponsive session
- restarting the machine
- putting a machine into maintenance mode
- resetting the user profile

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot applications

Application Analytics

The **Applications** view displays application-based analytics in a single, consolidated view to help analyze and manage application performance efficiently. You can gain valuable insight into the health and usage information of all applications published on the site. The default view helps identify the top running applications. This feature requires VDAs Version 7.15 or later.



The **Instances** column displays usage of the applications. It indicates the number of application instances currently running (both connected and disconnected instances). To troubleshoot further, click the **Instances** field to see the corresponding **Application Instances** filters page. Here, you can select application instances to log off or disconnect.

NOTE:

For custom scope administrators, Monitor does not display application instances created under application groups. To view all application instances, you must be a full administrator. For more information, see Knowledge Center article CTX256001.

Monitor the health of published applications in your site with the **Application Faults** and the **Application Errors** columns. These columns display the aggregated number of faults and errors that have occurred while launching the corresponding application in the last one hour. Click the **Application Faults** or **Application Errors** field to see failure details on the **Trends** \> **Application Failures** page corresponding to the selected application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The application failure policy settings govern the availability and display of faults and errors. For more information about the policies and how to modify them, see Policies for application failure monitoring in Monitoring policy settings.

Real-time application monitoring

You can troubleshoot applications and sessions by using the idle time metric to identify instances that are idle beyond a specific time limit.

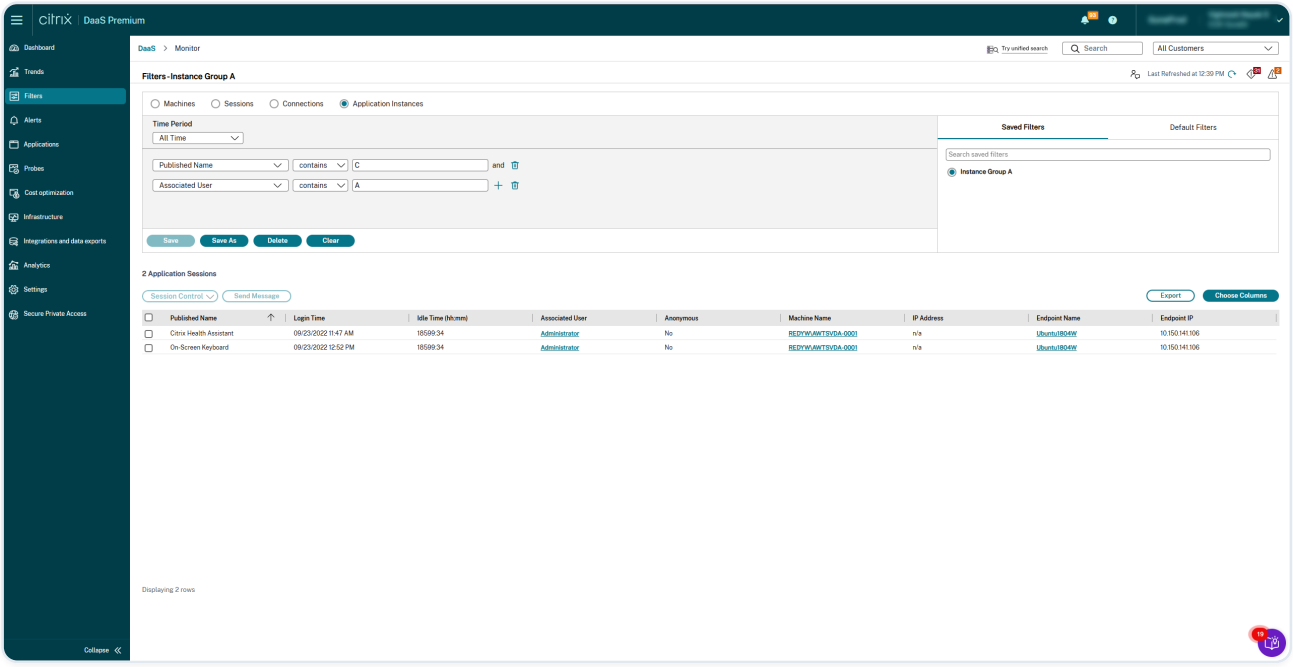
Typical use cases for application-based troubleshooting are in the healthcare sector, where employees share application licenses. There, you must end idle sessions and application instances to purge the Citrix Virtual Apps and Desktops™ environment, to reconfigure poorly performing servers, or to maintain and upgrade applications.

The **Application Instances** filter page lists all application instances on VDAs of Multi-session and Single session OS. The associated idle time measurements are displayed for application instances on VDAs of Multi-session OS that have been idle for at least 10 minutes.

NOTE:

The Application Instances metrics are available on sites of all license editions.

Use this information to identify the application instances that are idle beyond a specific time period and log off or disconnect them as appropriate. To do this, select **Filters \> Application Instances** and select a pre-saved filter or choose **All Application Instances** and create your own filter.



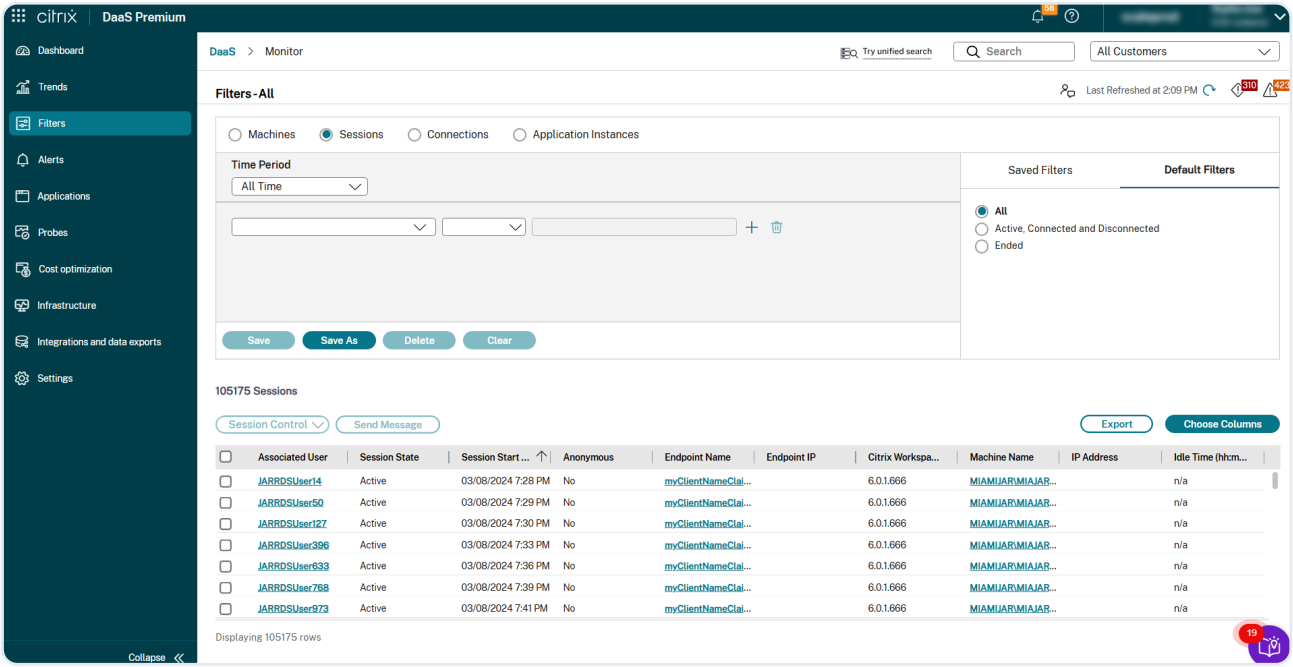
© 1997–2026 Citrix Systems, Inc. All rights reserved.

An example of a filter would be as follows. As **Filter by** criteria, choose **Published Name** (of the application) and **Idle Time**. Then, set **Idle Time** to **greater than or equal to** a specific time limit and save the filter for reuse. From the filtered list, select the application instances. Select option to send messages or from the **Session Control** drop-down, choose **Logoff** or **Disconnect** to end the instances.

NOTE:

Logging off or disconnecting an application instance logs off or disconnects the current session, thereby ending all application instances that belong to the same session.

You can identify idle sessions from the **Sessions** filter page using the session state and the session idle time metric. Sort by the **Idle Time** column or define a filter to identify sessions that are idle beyond a specific time limit. Idle time is listed for sessions on VDAs of Multi-session OS that have been idle for at least 10 minutes.



The **Idle time** is displayed as **N/A** when the session or application instance

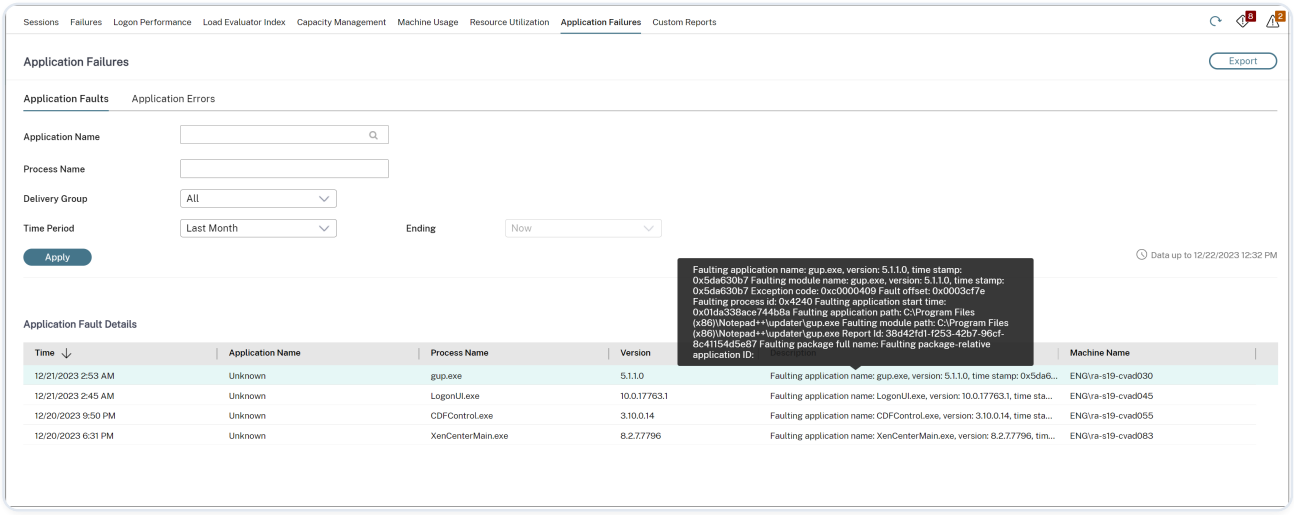
- has not been idle for more than 10 minutes,
- is launched on a VDA of Single session OS, or
- is launched on a VDA running Version 7.12 or earlier.

Historical application failure monitoring

The **Trends** -\> **Application Failures** tab displays failures associated with the published applications on the VDAs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about the availability of the application failure trends, see Data granularity and retention article. The application failures that are logged to the Event Viewer with source "Application Errors" are monitored. Click **Export** to generate reports in CSV, Excel, or PDF formats



The failures are displayed as **Application Faults** or **Application Errors** based on their severity. The Application Faults tab displays failures associated with loss of functionality or data. Application Errors indicate problems that are not immediately relevant; they signify conditions that might cause future problems.

You can filter the failures based on **Published Application Name**, **Process Name** or **Delivery Group,** and **Time Period.** The table displays the fault or error code and a brief description of the failure. The detailed failure description is displayed as a tooltip.

NOTE:

The Published Application name is displayed as “Unknown” when the corresponding application name cannot be derived. This typically occurs when a launched application fails in a desktop session or when it fails due to an unhandled exception caused by a dependent executable.

By default, only faults of applications hosted on Multi-session OS VDAs are monitored. You can modify the monitoring settings through the Monitoring Group Policies: Enable monitoring of application failures, Enable monitoring of application failures on Single session OS VDAs, and List of applications excluded from failure monitoring. For more information, see Policies for application failure monitoring in Monitoring policy settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application probing

Application probing automates the process of checking the health of Citrix Virtual Apps that are published in a site. The results of application probing are available in the **Monitor** console of Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service). Citrix Probe Agent supports sites hosted on Citrix Cloud Japan and Citrix Cloud Government Control Planes.

Ensure that the endpoint machines running probe agents are Windows machines with Citrix Receiver for Windows Version 4.8 or later, or Citrix Workspace app for Windows (formerly Citrix Receiver for Windows) Version 1808 or later. Workspace app for Unified Windows Platform (UWP) is not supported.

Requirements:

- Endpoint machines running probe agents are Windows machines with Citrix Receiver for Windows Version 4.8 or later, or Citrix Workspace app for Windows (formerly Citrix Receiver for Windows) Version 1906 or later. Workspace app for Unified Windows Platform (UWP) is not supported.
- Citrix Probe Agent supports the default form-based authentication as supported by Citrix® StoreFront Cloud. Citrix Probe Agent doesn't support other authentication methods like Single Sign-On (SSO) or Multi Factor Authentication (MFA). Similarly, Citrix Probe Agent works only when there is no proxy server or load balancer like Citrix Gateway or Citrix ADC deployed.
- Ensure that Microsoft .NET Framework version 4.7.2 or later is installed on the endpoint machine where you want to install the Probe Agent.
- To use the probing agent in Citrix Cloud Japan Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" to 2. To use the probing agent in Citrix Cloud Government Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" to 3.

User accounts/permissions required to run Application Probing are as follows:

- A unique user to probe on each endpoint machine. The user is not required to be an administrator; the probes can run in a non-admin context.
- User accounts with Windows administrator permissions to install and configure the Citrix Probe Agent on the endpoint machines
- A full administrator user account with the following permissions. Reusing existing user accounts for application probing might log off from the users' active sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Delivery group permissions:
  - Read-only
- Director permissions:
  - Create\\Edit\\Remove Probe Configurations
  - View Configurations page
  - View Trends page

Configure Application Probing

Configure your application probes to run during off-peak hours across multiple geographies. The comprehensive probe results can help to troubleshoot issues related to the applications, hosting machine or connection before the users experience them.

Citrix Probe Agent version 2103 supports site aggregation. Applications and desktops can be enumerated and launched from aggregated sites. When you configure the probe agent, select the **Workspace (StoreFront) Site Aggregation Enabled** option to enable enumeration of applications and desktops from aggregated sites. The following combinations of sites are supported:

- Multiple on-premises sites having one store URL.
- On-premises and cloud sites having either an on-premises store URL or a cloud store URL.
- Multiple cloud sites having one store URL.

NOTE:

You must create separate administrators or users to configure probes that have access to only one site.

STEP 1: INSTALL AND CONFIGURE THE CITRIX PROBE AGENT

The Citrix Probe Agent is a Windows executable that simulates the actual application launch by the user through Citrix Workspace app. It tests application launches as configured in Monitor and reports back the results to Monitor.

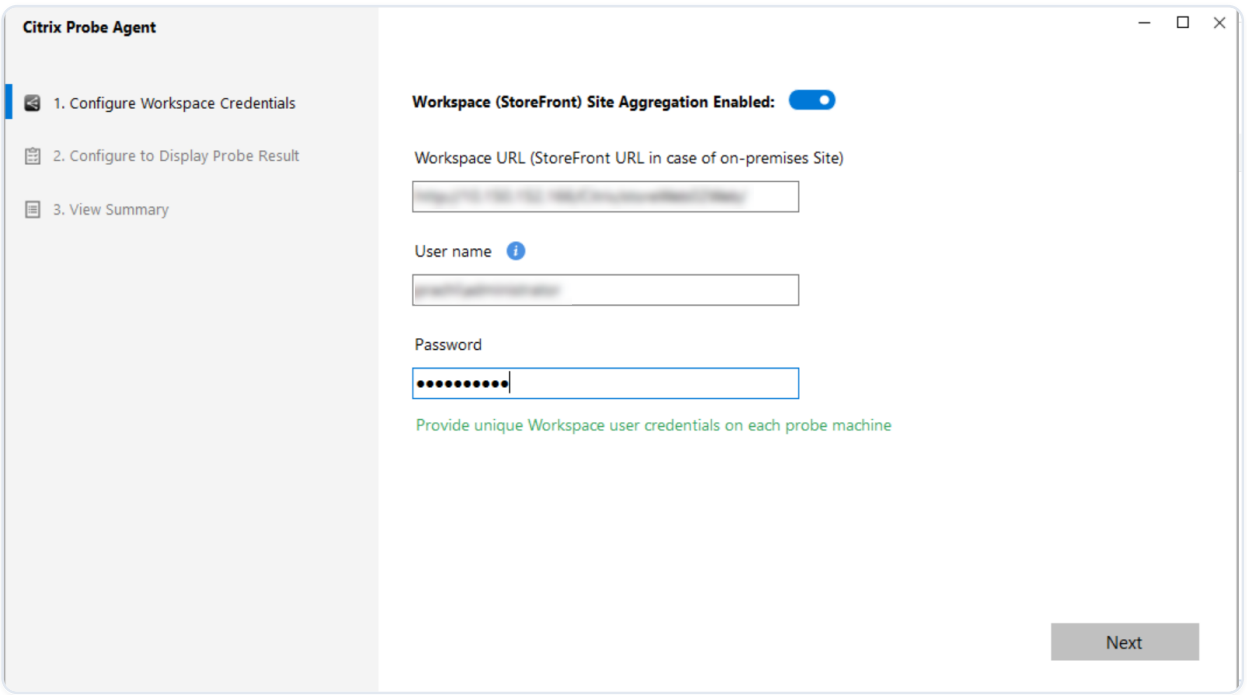
1. Identify endpoint machines from where you want to run application probing.
2. Users with administrative privileges can install and configure the Citrix Probe Agent on the endpoint machine. Download the Citrix Probe Agent executable available at `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/edition-software/premium-2411.html>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Start the agent and enter the credentials for the user the probe should log in as. Configure a unique user on each endpoint machine. The credentials are encrypted and stored securely.

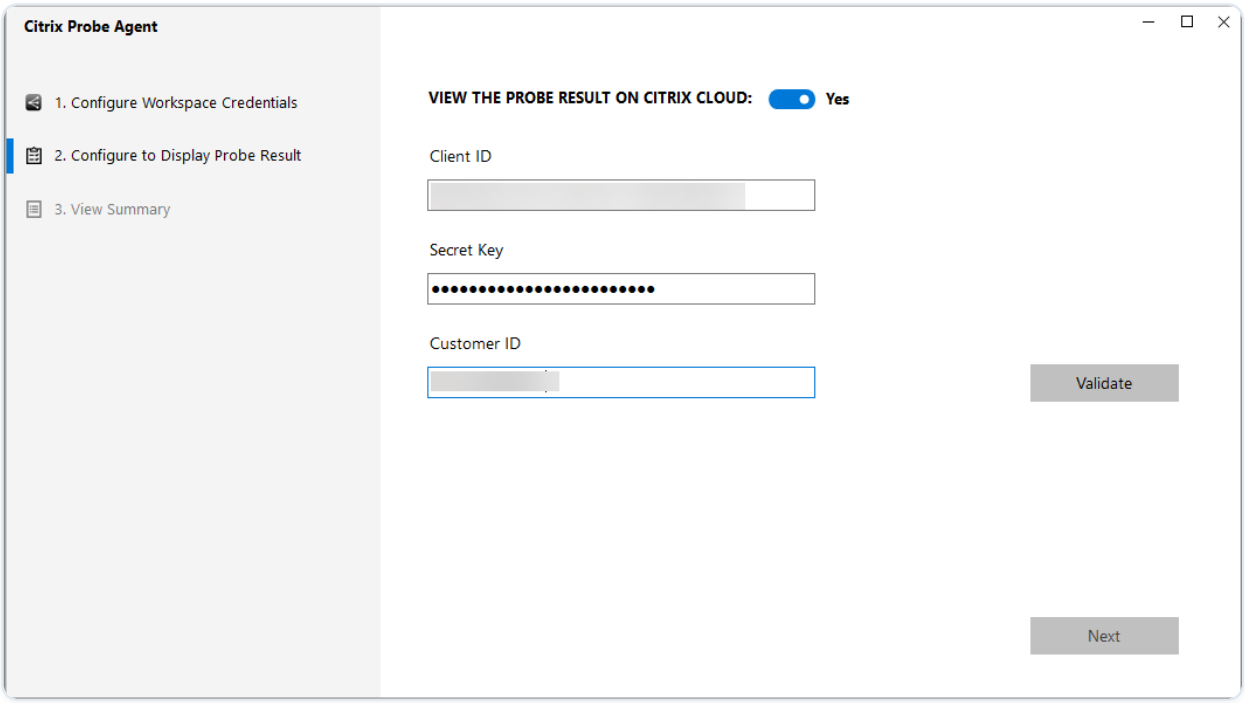
NOTES:

- To access the site to be probed from outside the network, type the login URL for Citrix Gateway in the **store URL** field. Citrix Gateway automatically routes the request to the corresponding site store URL.
- Use NetBIOS as the domain name in the user name field. For example, NetBIOS/username.
- App probing supports Citrix Content Collaboration™ service using authentication (AD only).



4. On the **Configure To Display Probe Result** tab, enter credentials to access Citrix DaaS. You can find the Customer Name or Customer ID, Client ID, and Secret Key from the API Access page in the Citrix Cloud™ console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

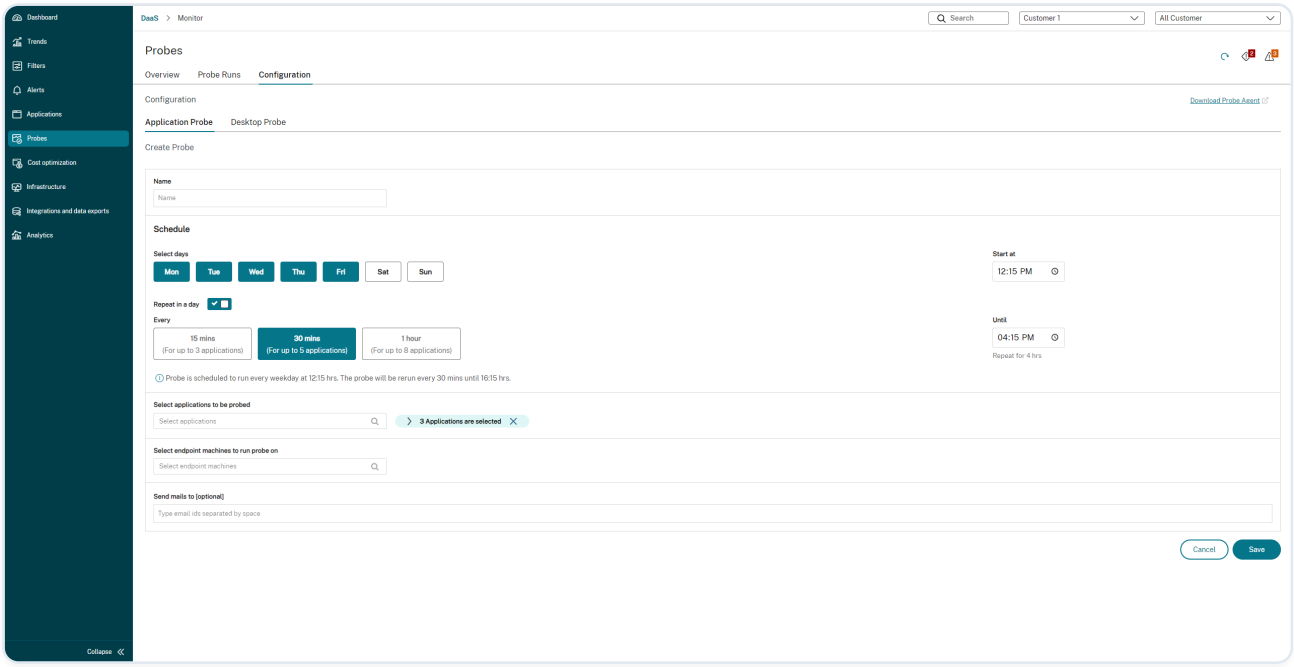


STEP 2: CONFIGURE APPLICATION PROBING IN THE MONITOR TAB

1. In Citrix DaaS, go to **Configuration** \> **Probe Configuration** \> **Application Probe** and click **Create Probe**:
2. In the **Create Probe** page, enter the name of the probe.
3. Select the schedule:
    a. Choose the days of the week on which you want the probe to run.
    b. Enter the start time at which you want the probe to run.
    c. In addition, you can choose the **Repeat in a day** option. Enter the end time and the interval in which you want the probe to repeat within a day. For example, the configuration below helps run application probes from 12:08 hours until 16:34 hours repeating every 30 minutes every Monday, Wednesday, Thursday, and Sunday.
4. Select the recommended number of applications to be probed depending on the interval.
5. Select the endpoint machines on which the probe must run.
6. Enter the email addresses to which the failure probe results are sent and click **Save**.

In this configuration, the application sessions launch at 12:08 hours, 12:38 hours, 13:08 hours, and so on until 16:08 hours every Monday, Wednesday, Thursday, and Sunday.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

- Configure your email server in **Alerts** > **Email Server Configuration**.
- After configuration in the **Monitor** console, the agent runs configured probes starting the next hour.
- The probes that were set up before the **Repeat in a day** option was introduced continue to run at their scheduled time. They have the **Repeat in a day** option disabled by default.

STEP 3: PROBE EXECUTION

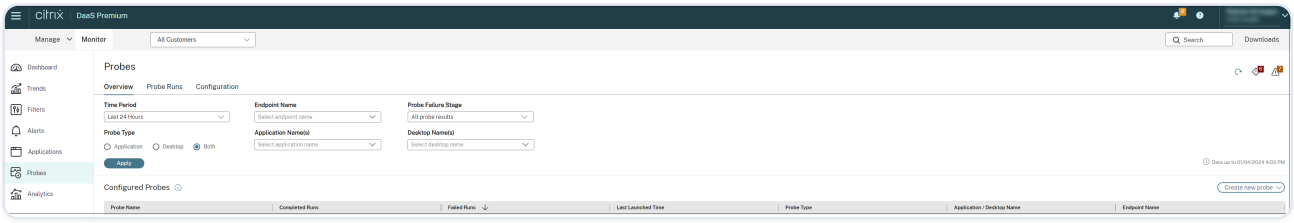
The agent runs application probing as per the probe configuration it fetches from Monitor every hour. It launches selected applications serially using Workspace. The agent reports the results back to Monitor via the Monitor database. Failures are reported in five specific stages:

- **Workspace Reachability** - configured store URL is not reachable.
- **Workspace Authentication** - configured credentials are invalid.
- **Workspace Enumeration** - Enumerate applications list does not contain the application to be probed.
- **ICA® download** - the ICA file is not available.
- **Application launch** – the application cannot be launched.

STEP 4: VIEW PROBE RESULTS

You can view the latest probe results in Citrix DaaS™ > **Applications** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To troubleshoot further, click the probe result link to see more details on the **Trends** \> **Application Probe Results** page.

The consolidated probe results data is available for the last 24 hours or last 7 days time periods on this page. You can see the stage in which the probe failed. You can filter the table for a specific application, probe failure stage, or endpoint machine.

Desktop probing

Desktop probing automates the process of checking the health of Citrix Virtual Desktops™ that are published in a site. The results of desktop probing are available in Monitor. Citrix Probe Agent now supports sites hosted on Citrix Cloud Japan and Citrix Cloud Government Control Planes.

In Monitor's Configuration page, configure the desktops to be probed, the endpoint machines to run the probe on, and the probe time. The agent tests the launch of selected desktops using Citrix Workspace app and reports the results back to Monitor. The probe results are displayed on the Monitor UI – the last 24-hours' data on the Applications page and historical probe data on the **Trends > Probe Results > Desktop Probe Results** page.

Here, you can see the stage when the probe failure occurred - Workspace Reachability, Workspace Authentication, Workspace Enumeration, ICA® download, or Desktop launch. The failure report is sent to the configured email addresses.

You can schedule your desktop probes to run during off-peak hours across multiple geographies. The comprehensive results can help to proactively troubleshoot issues related to provisioned desktops, hosting machines or connections before the users experience them.

This feature requires Probe Agent 1903 or later.

Requirements:

- Endpoint machines running probe agents are Windows machines with Citrix Receiver for Windows Version 4.8 or later, or Citrix Workspace app for Windows (formerly Citrix Receiver for Windows) Version 1906 or later. Workspace app for Unified Windows Platform (UWP) is not supported.
- Citrix Probe Agent supports the default form-based authentication as supported by StoreFront and StoreFront Cloud. Citrix Probe Agent doesn't support other authentication methods like

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Single Sign-On (SSO) or Multi Factor Authentication (MFA). Similarly, Citrix Probe Agent works only when there is no proxy server or load balancer like Citrix Gateway or Citrix ADC deployed.

- Ensure that Microsoft .NET Framework version 4.7.2 or later is installed on the endpoint machine where you want to install the Probe Agent.
- To use the probing agent in Citrix Cloud Japan Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" to 2. To use the probing agent in Citrix Cloud Government Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" to 3.

User accounts or permissions required to run Desktop probing:

- A unique user to probe on each endpoint machine. The user need not be an administrator; the probes can run in a non-admin context.
- User accounts with Windows administrator permissions to install and configure the Citrix Probe Agent on the endpoint machines
- A full administrator user account or a custom role with the following permissions. Reusing normal user accounts for desktop probing might log off the users' from the active sessions.
    - Delivery group permissions:
        - Read-only
    - Monitor permissions:
        - Create, Edit, Remove Alert Email Server Configuration - if the email server is not already configured
        - Create, Edit, Remove Probe Configurations
        - View Configurations page
        - View Trends page

Configure desktop probing

You can schedule your desktop probes to run during off-peak hours across multiple geographies. The comprehensive probe results can help to troubleshoot issues related to the desktops, hosting machine or connection before the users experience them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Probe Agent version 2103 supports site aggregation. Applications and desktops can be enumerated and launched from aggregated sites. When you configure the probe agent, select the **Workspace (StoreFront) Site Aggregation Enabled** option to enable enumeration of applications and desktops from aggregated sites. The following combinations of sites are supported:

- Multiple on-premises sites having one store URL.
- On-premises and cloud sites having either an on-premises store URL or a cloud store URL.
- Multiple cloud sites having one store URL.

NOTE:

You must create separate administrators or users to configure probes that have access to only one site.

STEP 1: INSTALL AND CONFIGURE THE CITRIX PROBE AGENT

The Citrix Probe Agent is a Windows executable that simulates the actual desktop launch by the user through Workspace. It tests desktop launches as configured in Monitor and reports back the results to Monitor.

1. Identify endpoint machines from where you want to run desktop probing.
2. Users with administrative privileges can install and configure the Citrix Probe Agent on the endpoint machine. Download the Citrix Probe Agent executable available at `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/edition-software/premium-2411.html>`
3. Start the agent and configure your Workspace Receiver for Web credentials. Configure a unique Workspace user on each endpoint machine. The credentials are encrypted and stored securely.

   NOTES:

   - To access the site to be probed from outside the network, type the Citrix Gateway login page URL on the store URL field. Citrix Gateway automatically routes the request to the corresponding site store URL. This feature is available for Citrix Gateway version 12.1 or later.
   - Use NetBIOS as the domain name in the user name field. For example, NetBIOS/username.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Desktop probing supports Citrix Content Collaboration™ service using Workspace authentication (AD only).
- You must enable Interactive Logon for the configured unique StoreFront user.

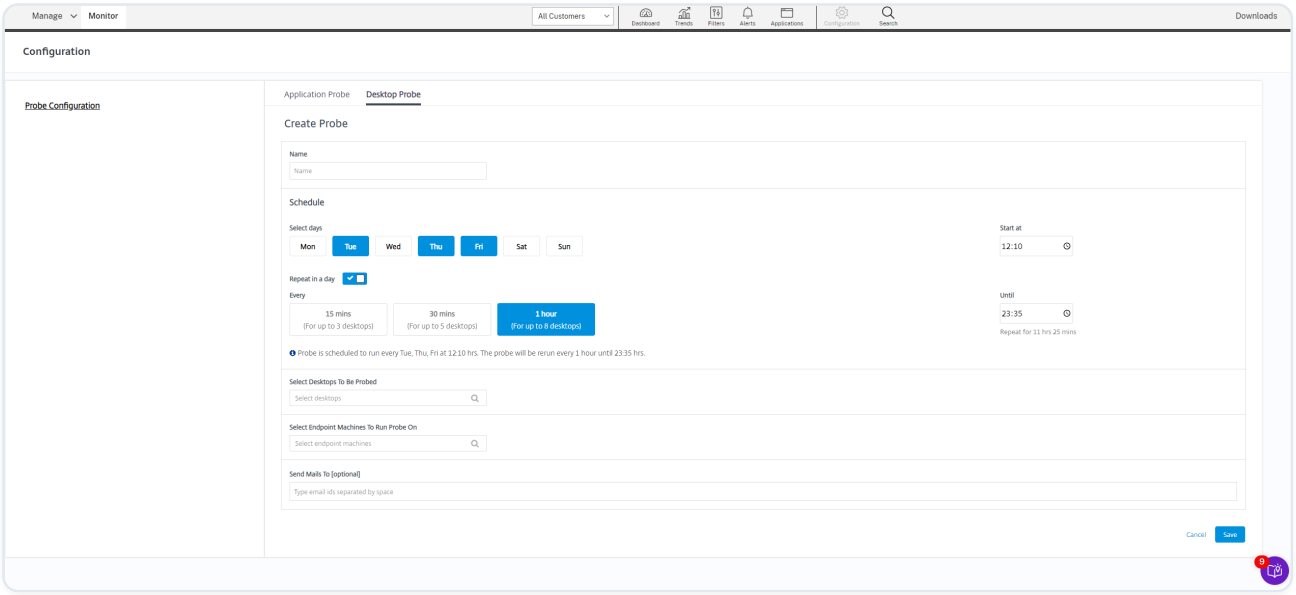
4. On the **Configure To Display Probe Result** tab, enter your Monitor credentials. You can find the Customer Name or Customer ID, Client ID, and Secret Key from the API Access page in the Citrix Cloud™ console.

STEP 2: CONFIGURE DESKTOP PROBING IN MONITOR

1. In Citrix DaaS, go to **Configuration** \> **Probe Configuration** \> **Application Probe** and click **Create Probe**.
2. In the **Create Probe** page, enter the name of the probe.
3. Select the schedule:
    a. Choose the days of the week on which you want the probe to run.
    b. Enter the start time at which you want the probe to run.
    c. In addition, you can choose the **Repeat in a day** option. Enter the end time and the interval in which you want the probe to repeat within a day. For example, the configuration below helps run desktop probes from 12:10 hours until 23:35 hours repeating every hour every Tuesday, Thursday, and Friday.
4. Select the recommended number of desktops to be probed depending on the interval.
5. Select the endpoint machines on which the probe must run.
6. Enter the email addresses to which the failure probe results are sent and click **Save**.

In this configuration, the desktop sessions launch at 12:10 hours, 13:10 hours, 14:10 hours, and so on until 23:10 hours every Tuesday, Thursday, and Friday.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

- Configure your email server in **Alerts** > **Email Server Configuration**.
- After desktop probing configuration is complete, the agent runs the configured probes starting the next hour.
- The probes that were set up before the **Repeat in a day** option was introduced continue to run at their scheduled time. They have the **Repeat in a day** option disabled by default.

STEP 3: PROBE EXECUTION

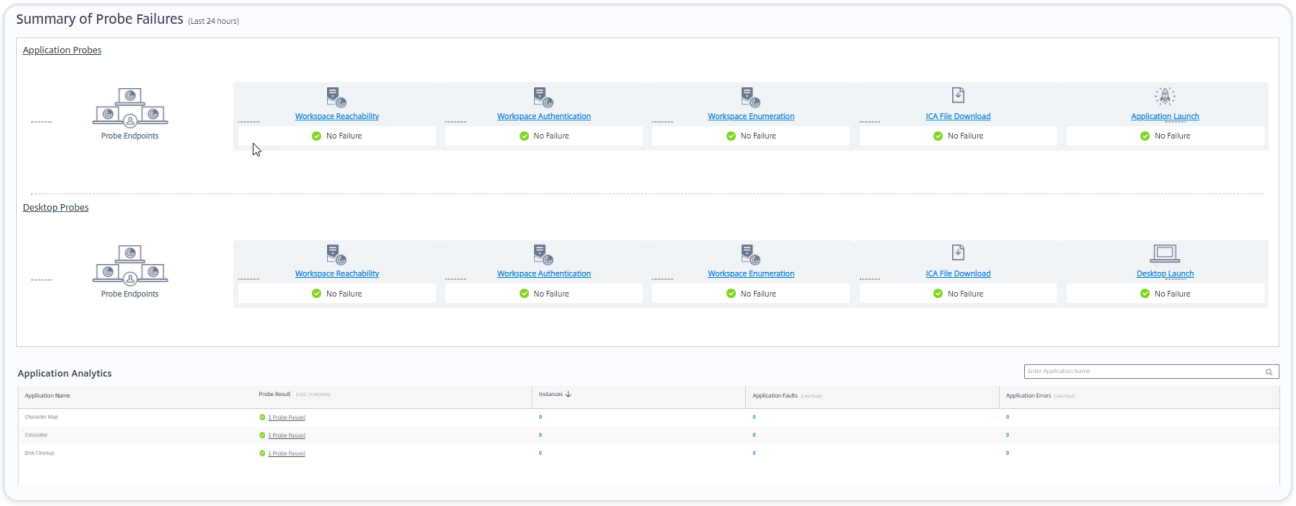
The agent runs desktop probing as per the probe configuration it fetches from Monitor periodically. It launches selected desktops serially using Workspace. The agent reports the results back to Monitor via the Monitor database. Failures are reported in five specific stages:

- **Workspace Reachability** - configured store URL is not reachable.
- **Workspace Authentication** - configured credentials are invalid.
- **Workspace Enumeration** - Enumerate desktops list does not contain the desktop to be probed.
- **ICA download** - the ICA file is not available.
- **Desktop launch** – the desktop cannot be launched.

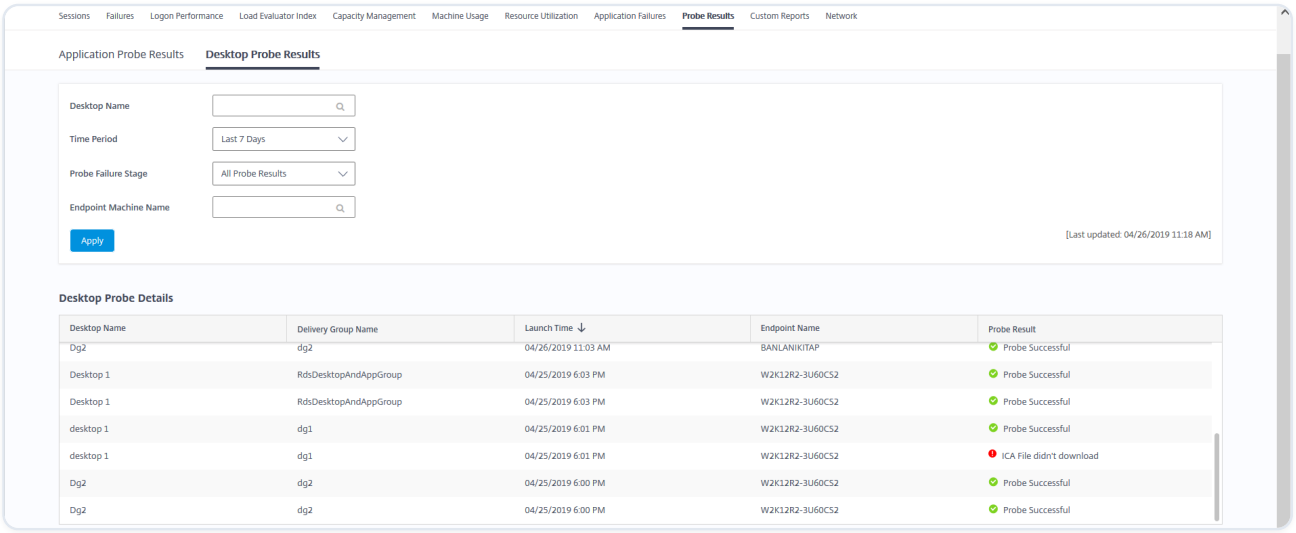
STEP 4: VIEW PROBE RESULTS

You can view the latest probe results on the **Desktops** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To troubleshoot further, click the probe result link to see more details on the **Trends** >**Probe Results** > **Desktop Probe Results** page.



The consolidated probe results data is available for the last 24 hours or last 7 days time periods on this page. You can see the stage in which the probe failed. You can filter the table for a specific desktop, probe failure stage, or endpoint machine.

Machine health monitoring

1. Introduction: What's New?

To provide richer insights into the health and performance of Virtual Delivery Agent (VDA) machines, we've introduced several key enhancements:

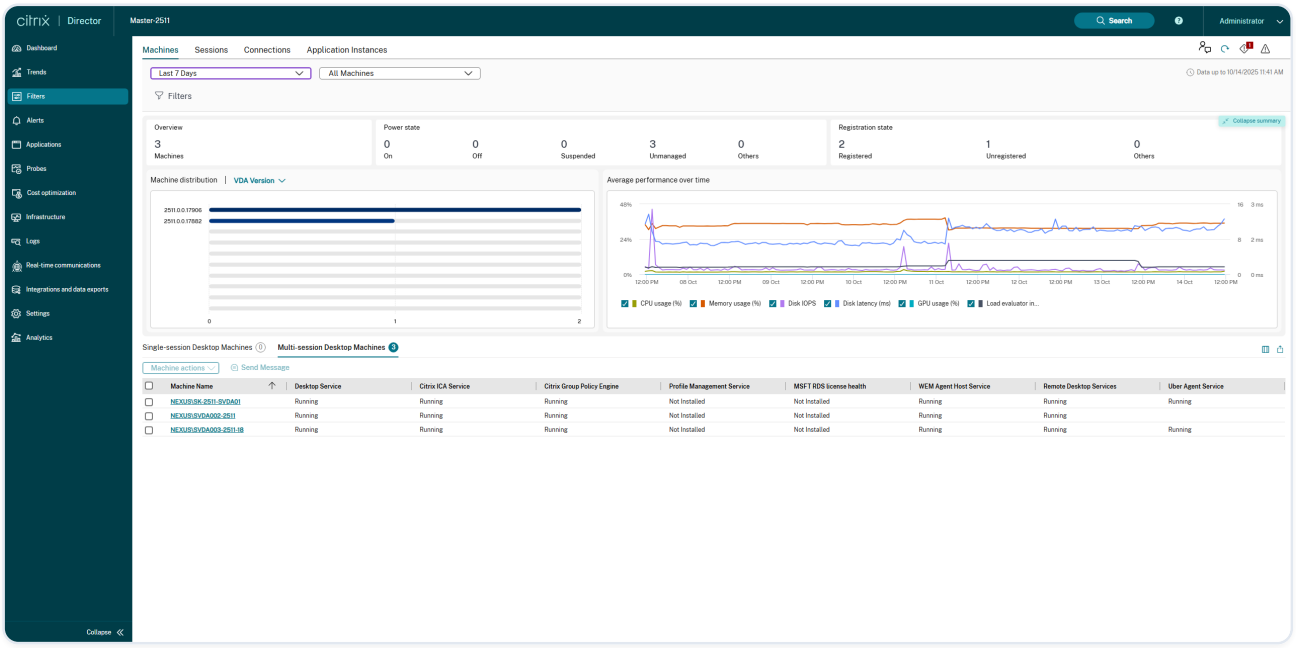
- **New Visualizations:**

  a. A Summary Panel has been added with three categories: **Overview, Power State** and **Registration State**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Two new charts, **Machine distribution** and **Average performance over time**, have been added to provide an immediate, graphical view of machine's status and historical trends.

- **Enhanced Tabular Data:** The **Single-session** and **Multi-session Desktop** Machines tables now include detailed status columns for critical VDA services, helping to quickly pinpoint the root cause of machine health issues.
- **New Time Range Filter:** Two new time range filters - Last 2 Hours and Last 7 Days has been added to provide support for historical trends.



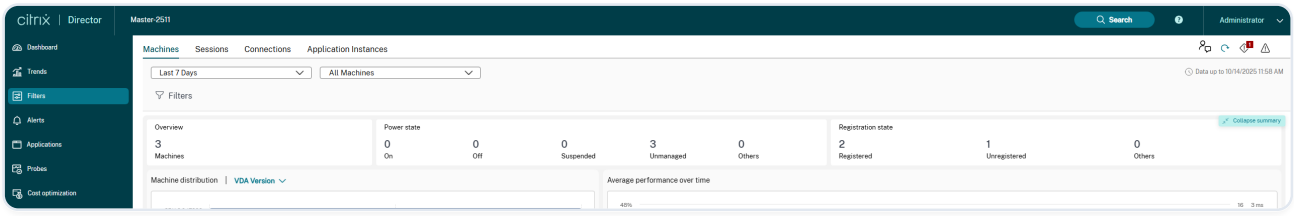
2. Understanding the New Visualizations

2.1. Summary Panel

- **Overview:** Displays the total number of VDAs (Machines) associated.
- **Power State:** Displays the number of machines based on their power states - On, Off, Suspended, Unmanaged and Others.
- **Registration State:** Displays the number of machines based on their registration states - Registered, Unregistered and Others.

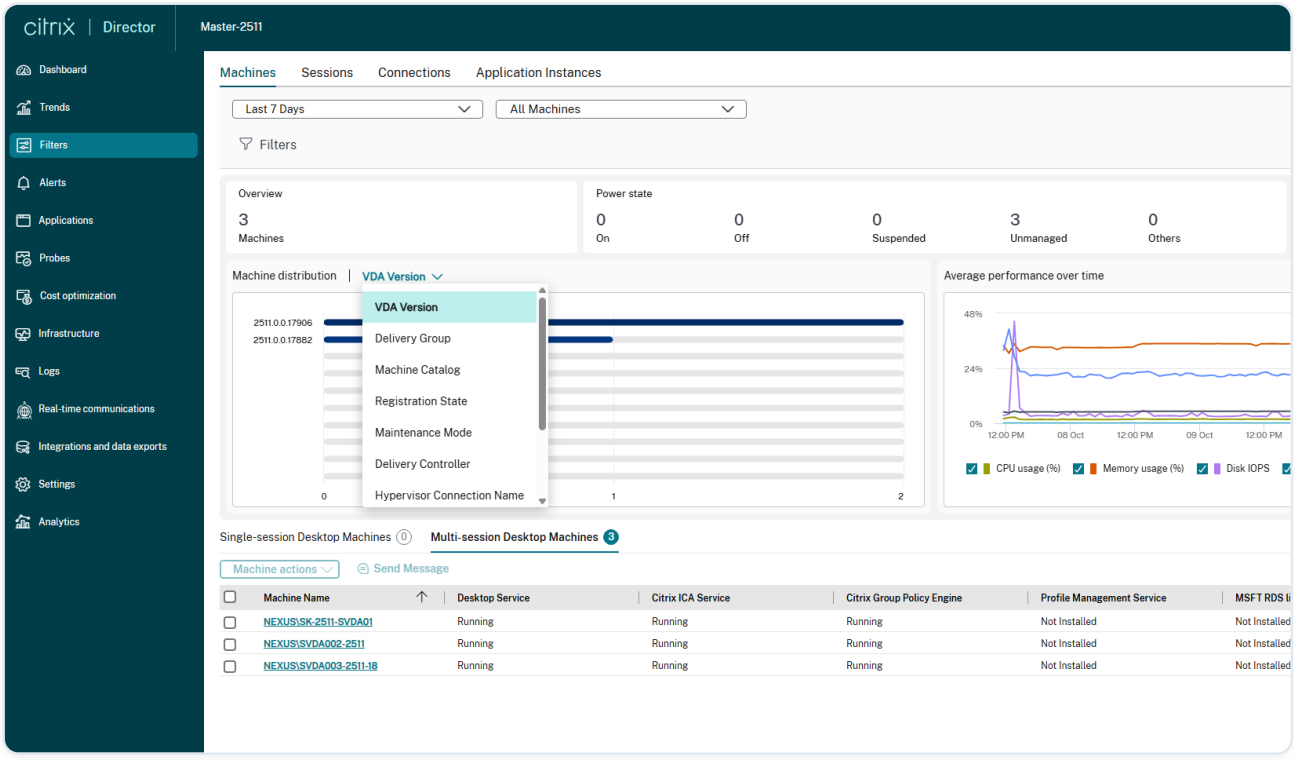
This summary is collapsible and helps admins to take neccessary actions based on the above seggreation like switching on machines which are in Off state or to identify which machines are in Unregistered states.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

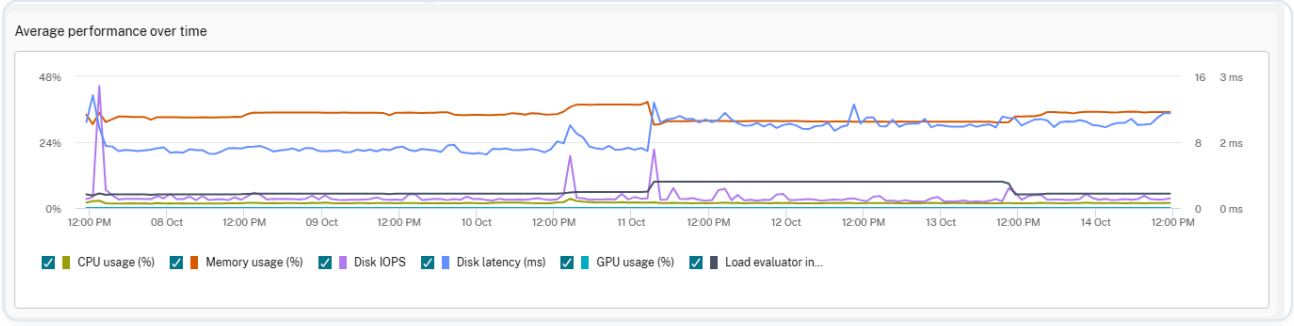


2.2. Machine Distribution

- **Purpose:** This bar chart provides a quick, visual breakdown of the VDA machines included in the current filter set. The default filter is set to VDA Version. However the user can filter using Delivery Group, Machine Catalog, Registration State, Maintenance Mode, Delivery Controller, Hypervisor Connection Name, Failure Type, Failure Reason and Power State
- **Utility:** This empowers admin to get the overall overview od the VDAs based on the filter criteria. For example, Machine Distribution on VDA Version helps administrators quickly identify if a significant portion of the VDAs is running an older or non-standard VDA version, which can be a prerequisite for troubleshooting or upgrade planning.



2.3. Average Performance Over Time

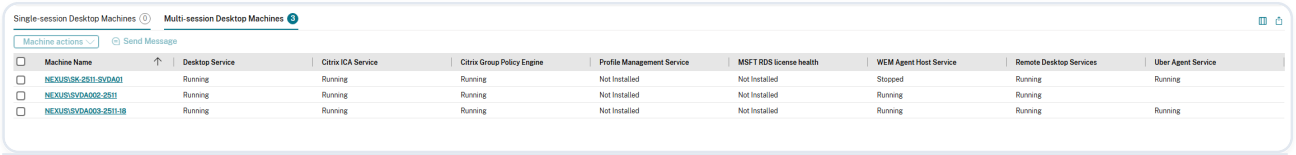


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Purpose:** This time-series chart tracks key performance metrics over the selected time range (e.g., Last 24 Hours).
- **Key Metrics Tracked:**
  - **CPU usage (%):** The average percentage of CPU being used.
  - **Memory usage (%):** The average percentage of RAM being utilized.
  - **Disk IOPS:** The average number of Input/Output Operations Per Second.
  - **Disk latency (ms):** The average time delay (in milliseconds) for disk I/O requests.
  - **GPU usage (%):** The average percentage of GPU being used (if applicable).
  - **Load Evaluator (%):** The calculated load index percentage on the VDA machine.
- **Utility:** Allows for historical trend analysis, helping to spot performance degradation, resource contention, and when peak loads occur.

3. Enhanced Tabular Data

Single/Multi-Session Table: New Column Definitions



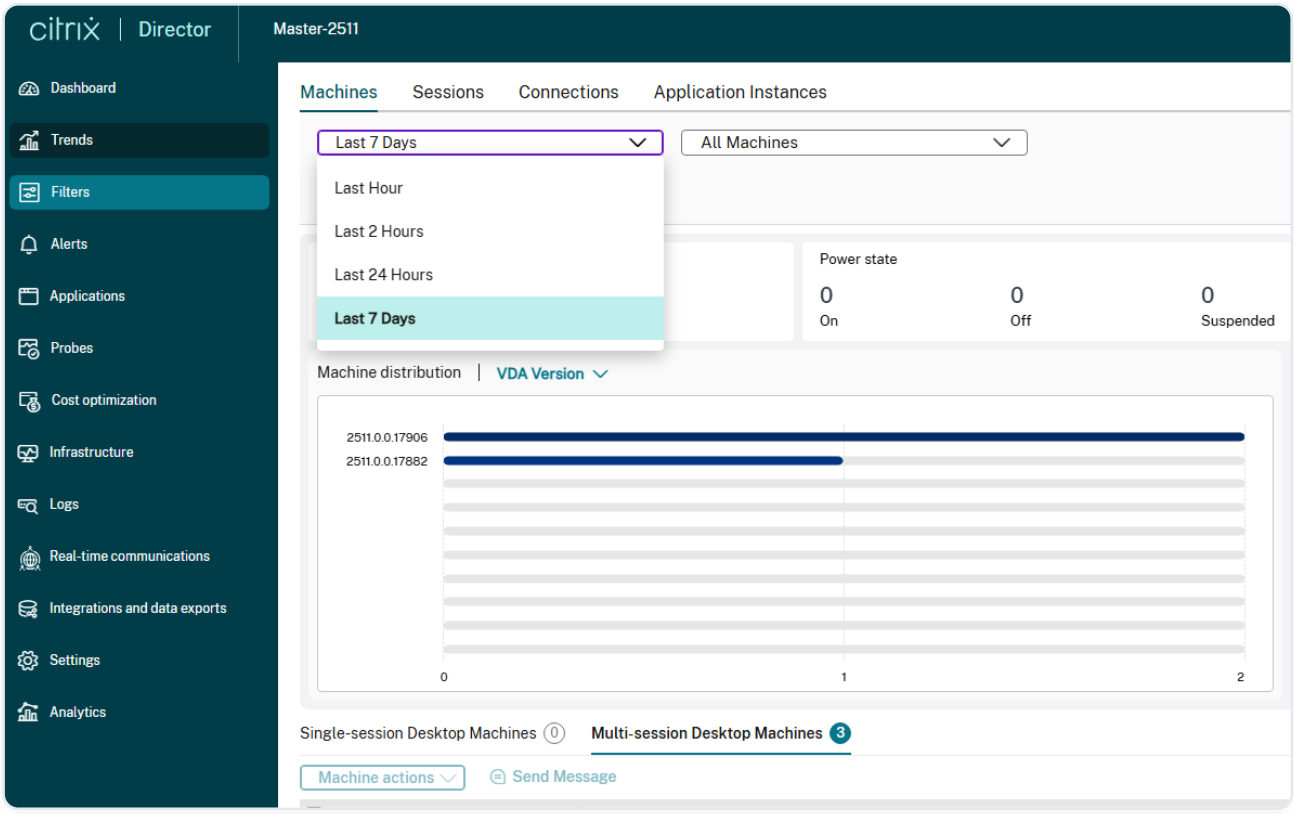
COLUMN NAME	DESCRIPTION	POSSIBLE VALUES
Desktop Service	Health status of the main service responsible for managing the desktop session (e.g., CtxSvcHost).	Running, Stopped, Not Installed, Paused, Start Pending, Stop Pending, Continue Pending, Pause Pending, Unknown
Citrix ICA Service	Health status of the core service that handles the Independent Computing Architecture (ICA) protocol for user sessions.	Running, Stopped, Not Installed, Paused, Start Pending, Stop Pending, Continue Pending, Pause Pending, Unknown
Citrix Group Policy Engine	Health status of the service responsible for processing and applying Citrix-specific policies.	Running, Stopped, Not Installed, Paused, Start Pending, Stop Pending, Continue Pending, Pause Pending, Unknown

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN NAME	DESCRIPTION	POSSIBLE VALUES
Profile Management Service	Health status of the Citrix Profile Management that is used for managing user profiles in Citrix virtual environments.	Running, Stopped, Not Installed, Paused, Start Pending, Stop Pending, Continue Pending, Pause Pending, Unknown
MSFT RDS license health	Indicates the status of the Microsoft Remote Desktop Services (RDS) licensing check.	Running, Stopped, Not Installed, Paused, Start Pending, Stop Pending, Continue Pending, Pause Pending, Unknown
WEM Agent Host Service	Health status of the Workspace Environment Management (WEM) agent responsible for optimization and configuration.	Running, Stopped, Not Installed, Paused, Start Pending, Stop Pending, Continue Pending, Pause Pending, Unknown
Remote Desktop Services	Health status of the underlying Microsoft Remote Desktop Services (required for both single and multi-session host functionality).	Running, Stopped, Not Installed, Paused, Start Pending, Stop Pending, Continue Pending, Pause Pending, Unknown
Uber Agent Service	Health status of the third-party monitoring agent service (if applicable and installed).	Running, Stopped, Not Installed, Paused, Start Pending, Stop Pending, Continue Pending, Pause Pending, Unknown

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Support for new Time Range Filters



1. **Last 2 Hours**

   - **Purpose:** Provides a high-granularity, immediate view of VDA resource utilization over the last 120 minutes.
   - **Utility:** This short time frame is ideal for real-time troubleshooting. Use it to pinpoint the exact time a resource spike (like high CPU or low disk IOPS) occurred and correlate it with recent user activity or administrative actions.

2. Last 7 Days

   - **Purpose:** Displays resource usage and performance trends over the past week.
   - **Utility:** This is the standard filter for weekly performance review. It helps administrators identify recurring performance issues, such as specific days or peak hours (e.g., Monday morning logons) that consistently stress VDA resources, allowing for proactive capacity planning and optimization.

VDA Health Monitoring Metrics: Supported platforms and versions

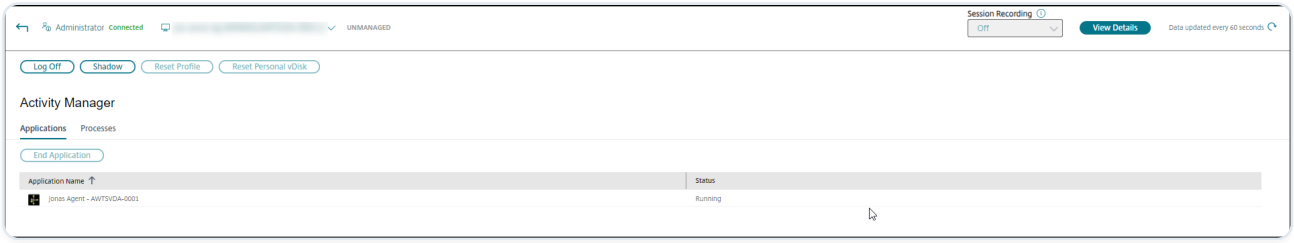
VDA COLUMNS	WINDOWS	MAC	LINUX
Desktop Service	2511 or above	2511 or above	2511 or above

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA COLUMNS	WINDOWS	MAC	LINUX
Citrix ICA Service	2511 or above	2511 or above	2511 or above
Citrix Group Policy Engine	2511 or above	2511 or above	2511 or above
Profile Management Service	2511 or above	2511 or above	2511 or above
MSFT RDS license health	2511 or above	2511 or above	2511 or above
WEM Agent Host Service	2511 or above	2511 or above	2511 or above
Remote Desktop Services	2511 or above	2511 or above	2511 or above
Uber Agent Service	2511 or above	2511 or above	2511 or above

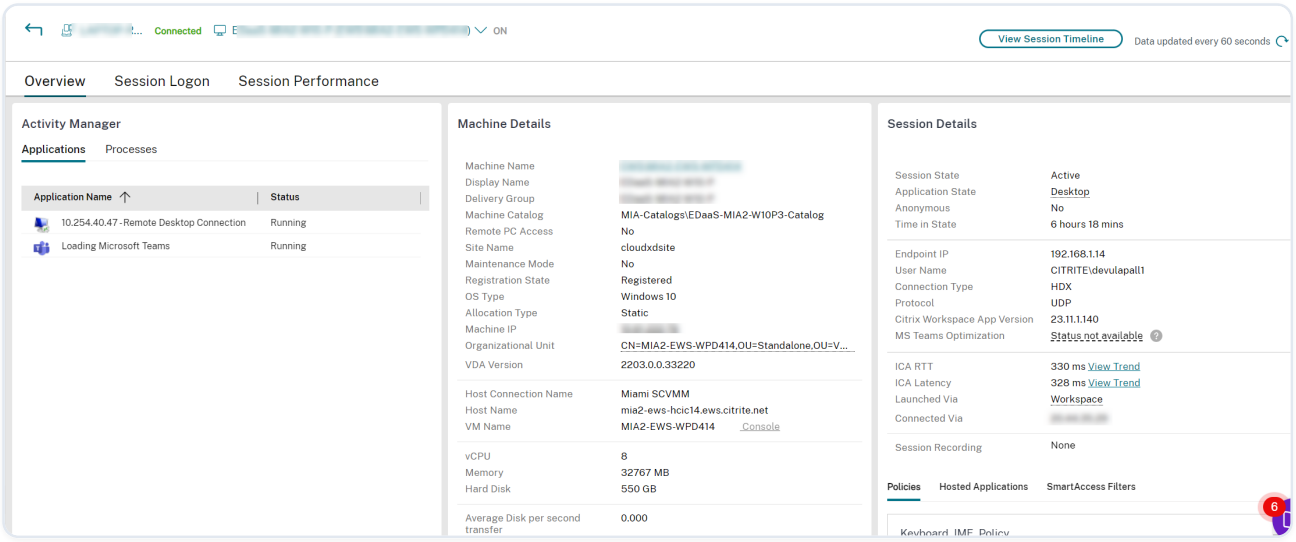
Troubleshoot user issues

Use the Monitor's **Help Desk** view (**Activity Manager** page) to view information about the user or endpoint.



Clicking **View Details** from the Activity Manager for User opens the **User Details** page. Clicking **View Details** from the Activity Manager for Endpoint opens the **Endpoint Details** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If the user had started more than one session, the session selector is displayed.



Choose a session to view the details.

- Check details about the session, user's sign in experience, session startup, connection, and applications.
- you can Shadow the user's machine.
- Troubleshoot the issue with the recommended actions in the following table, and, if needed, escalate the issue to the appropriate administrator.

Microsoft Teams optimization status

Citrix Monitor displays the Microsoft Teams optimization status for HDX™ sessions in the **User Details** page > **Session Details** panel > **MS Teams Optimization** field. Microsoft Teams being

© 1997–2026 Citrix Systems, Inc. All rights reserved.

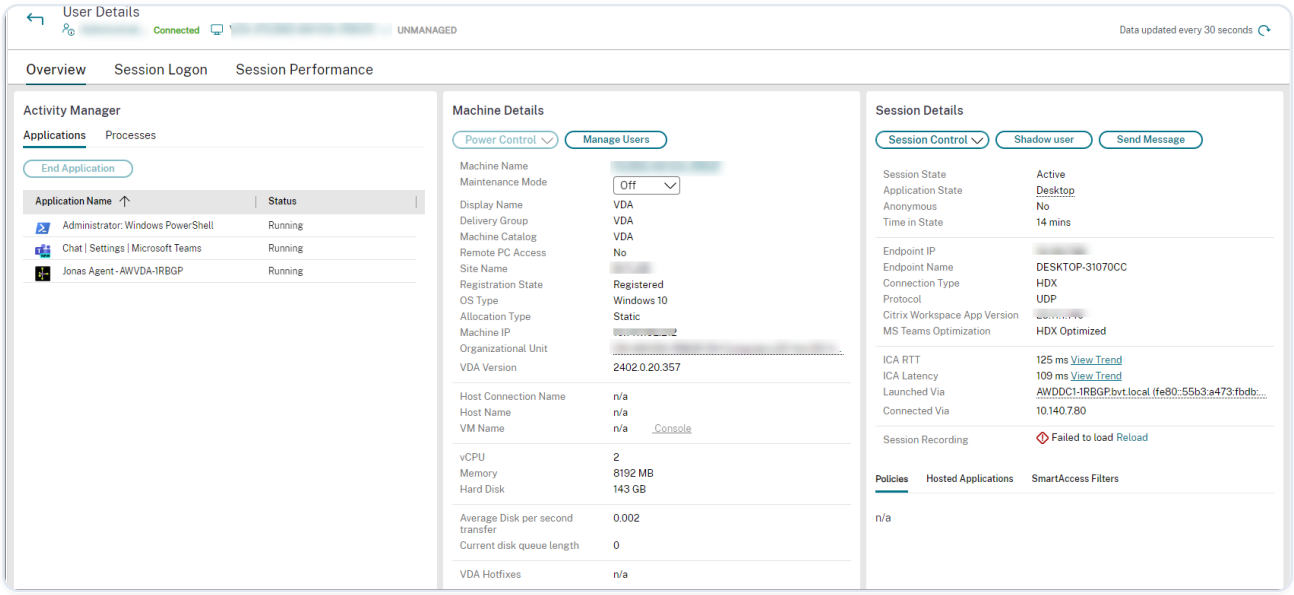
optimized is critical for the better user experience such as clear audio and video. Visibility of the Microsoft Teams optimization status is useful in reducing the time required to resolve tickets and helps administrators identify important metrics during troubleshooting.

NOTE:

Citrix Monitor supports Microsoft Teams version 2.1 or earlier.

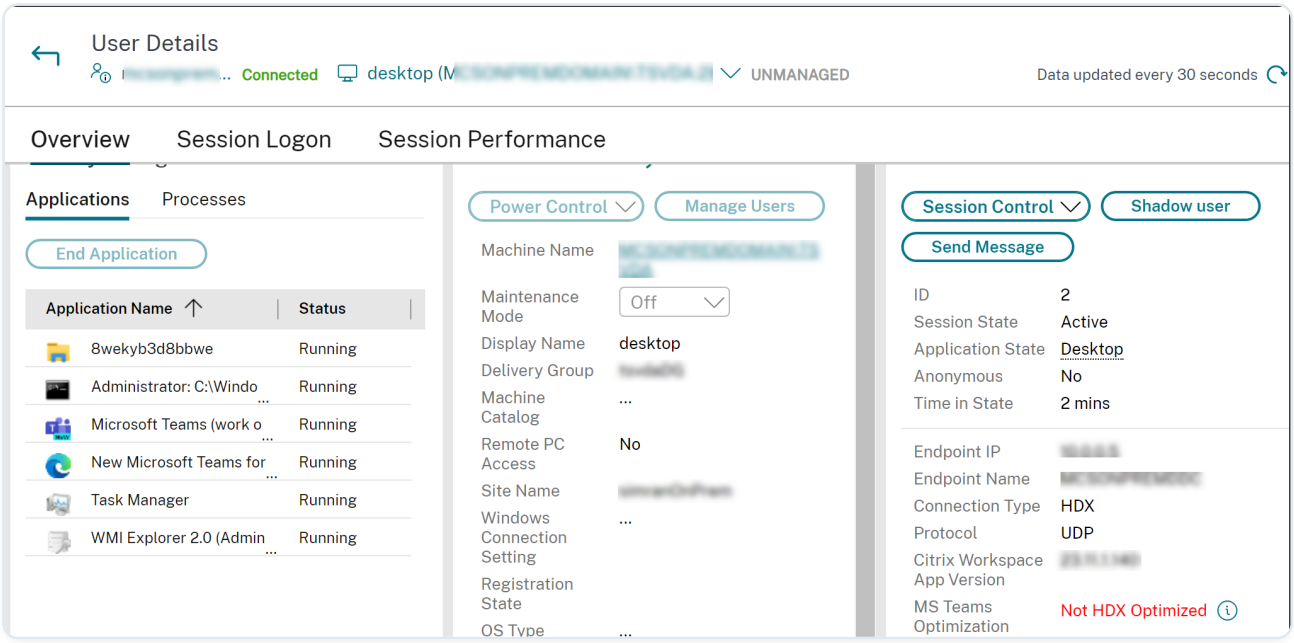
Prerequisites:

- VDA are running version 2311 and later.
- Citrix Workspace app versions supported are listed in Optimization for Microsoft Teams.
- Microsoft Teams runs as a published app or inside a published desktop.
- Crucial services such as the Citrix HDX HTML5 Video Redirection Service, are running.



If the Microsoft Teams isn't optimized, the tooltip provides a link to an external troubleshooting live article from HDX containing tips to optimize Microsoft Teams. Troubleshooting HDX Optimization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Troubleshooting tips

USER ISSUE	SUGGESTIONS
Logon takes a long time or fails intermittently or repeatedly	Diagnose user logon issues
Session startup takes a long time or fails intermittently or repeatedly	Diagnose session startup issues
Identify the components involved in establishing the session	Analyze the Session Topology view
Session response is slow or not responding	Diagnose session performance issues
Application is slow or not responding	Resolve application failures
Connection failed	Restore desktop connections
Session is slow or not responding	Restore sessions
Video is slow or poor quality	Run HDX channel system reports

NOTE:

To make sure that the machine is not in maintenance mode, from the User Details view, review the Machine Details panel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session Performance

The **Session Performance** tab has enhanced troubleshooting workflows starting with the ability to correlate real-time metrics in identifying issues within user sessions. The **Session Topology** panel provides a visual representation of the in-session path for connected HDX sessions. The **Performance Metrics** panel provides trends for the session metrics like ICARTT, ICA Latency, Frames Per Second, Output Bandwidth Available, and Output Bandwidth Consumed help indicate how these metrics have performed over time. For more information, see Diagnose session performance issues.

Search tips

Search for username is conducted across all configured Active Directories.

When you type a multiuser machine name in a Search field, the Machine Details for the specified machine are displayed.

When you type an endpoint name in a Search field, the unauthenticated (anonymous) and authenticated sessions that are connected to a specific endpoint are listed. This list enables troubleshooting unauthenticated sessions. Ensure that endpoint names are unique to enable troubleshooting of unauthenticated sessions.

The search results also include users who aren't currently using or assigned to a machine.

- Searches aren't case-sensitive.
- Partial entries produce a list of possible matches.
- After you type a few letters of a two-part name, separated by a space, the results include matches for both strings. The examples for two-part names are user name, family name and first name, or display name. For example, if you type "jo rob", the results might include strings such as “John Robertson” or "Robert Jones".

To return to the landing page, select **Manage > Monitor** in the left pane of Studio.

Diagnose conditional authentication failures

Conditional authentication allows Citrix Cloud admins to direct end users to different Identity Providers (IdPs) during the Workspace login flow based on policy conditions you set. This means different end users will have varying levels of access verification based on risk factors established by the Administrator. For more information on Conditional authentication, see Conditional authentication.

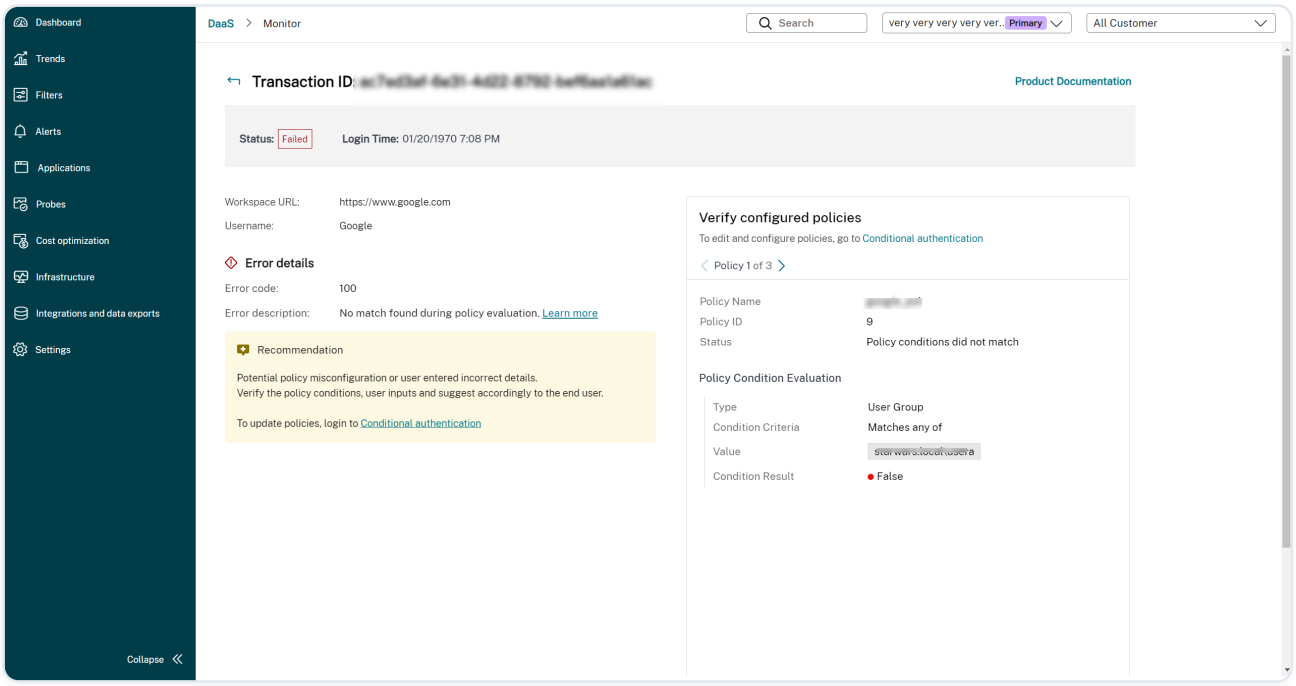
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Whenever any conditional authentication fails, you can use the transaction ID available in the failure message and search in the Monitor for the failure details. Monitor helps you to troubleshoot conditional authentication failure events by displaying failure reasons and conditional policies on the Monitor UI.

Viewing conditional authentication failures

To view the conditional authentication failure, follow these steps:

1. Copy the transaction ID for the failed session that uses conditional authentication.
2. On the Monitor dashboard, click **Search**.
3. Select **Transaction ID** from the drop-down list.
4. Paste the copied transaction ID. Click the search result and the transaction ID details page appears.



Transaction ID details

The following details are displayed on the Transaction ID details page:

FIELD	DESCRIPTION
Status	Displays the status of the conditional authentication. Possible values are *Success* or *Failed*.
Login Time	The time of the login.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD	DESCRIPTION
Workspace URL	The store URL added to Citrix Workspace™ app.
Error Details	
Error Code	Displays the error code. The possible error codes are
	100 - This error occurs when no match is found during policy evaluation.
	200 - This is an internal error. If the issue persists, contact Citrix® support team.
Error Description	Displays the description of the error.
Verify Configured Policies	
Policy Name	Displays the policy name.
Policy ID	Displays the policy ID.
Status	Displays the status of the policy.
Policy Condition Evaluation	
Type	Displays the policy condition type.
Condition Criteria	Displays the condition criteria.
Value	Displays the policy condition value.
Condition Result	Displays the result of the policy evaluation.

Diagnose Device Posture service transactions

Administrators can now diagnose and troubleshoot Device Posture Service transactions effectively. This update enhances troubleshooting capabilities in Citrix Monitor, providing detailed insights into Device Posture policy evaluation, compliance checks, and error diagnostics.

Understanding the Device Posture service evaluation flow

A typical Secure Private Access or VDI app access launch involves the following three stages:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Pre-authentication**: A basic endpoint hygiene check is conducted using Device Posture Service. Access is blocked before authentication if a device fails to meet compliance policies.
2. **Authentication**: Authenticates the user in this stage. Authentication fails if there is credential mismatches or identity provider errors.
3. **Application access**: The following two sub stages are involved in this stage:
    - **Policy brokering and enumeration stage**: When a user's device context violates policy settings, access to applications is restricted.
    - **Application launch stage**: The final stage, where an application transaction completes using Citrix Enterprise Browser™, Secure Private Access client, or native endpoint client.

Troubleshooting enhancements in Citrix Monitor

With this update, Citrix Monitor provides search-based Device Posture Service troubleshooting, allowing IT teams to:

- Filter transactions by a user ID or transaction ID for targeted debugging.
- Analyze policy evaluation outcomes such as whether a device is compliant, non-compliant, or blocked due to policy violations.
- Pinpoint policy failures by examining detailed compliance checks, expected values, and real-time contextual values.
- Review device metadata, policy configurations, and logs for deeper diagnostics.
- Identify failed transactions due to system errors, with error messages linked to knowledge-base articles for quick resolution.

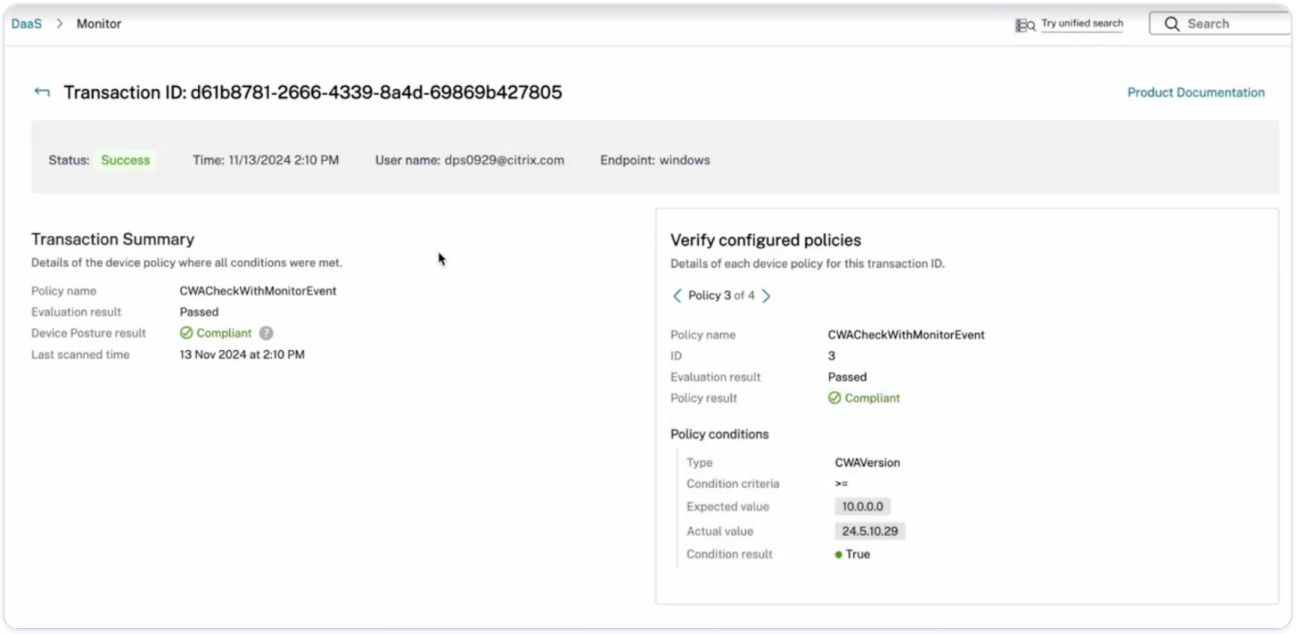
How IT teams can use the troubleshooting enhancement

TRIAGING DEVICE POSTURE ISSUES

Search a user-reported transaction ID to locate relevant Device Posture Service logs quickly. Review whether compliance checks passed or failed and determine root causes.

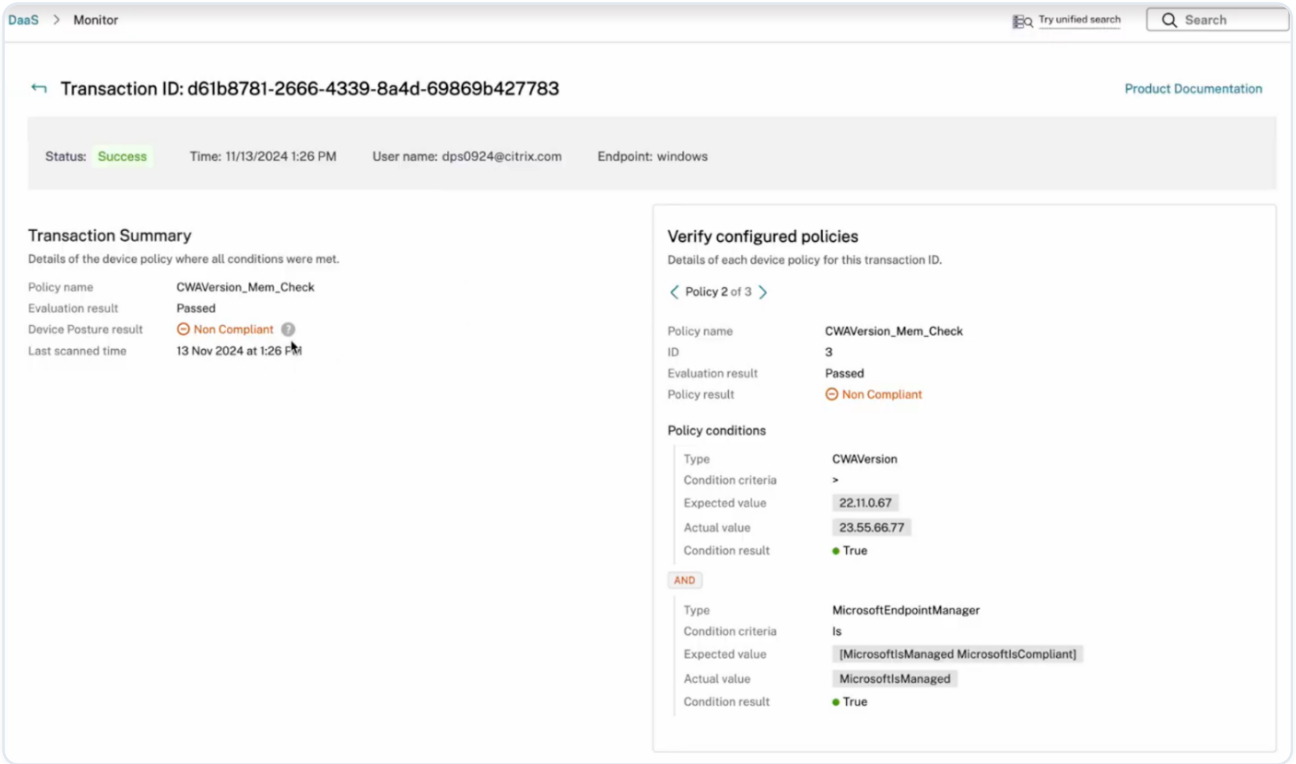
For example, when searching for a transaction ID, you can review the Device Posture check policy outcome—whether it was successful (compliant or non-compliant) or failed due to an error. The system provides the full context of the Device Posture Service evaluation, including client metadata, policy details, and other transaction details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



INVESTIGATING POLICY-BASED ACCESS BLOCKS

When a device is non-compliant, IT can inspect the exact policy parameters that failed. The system provides side-by-side comparisons of the configured expected value to the device's real-time data.

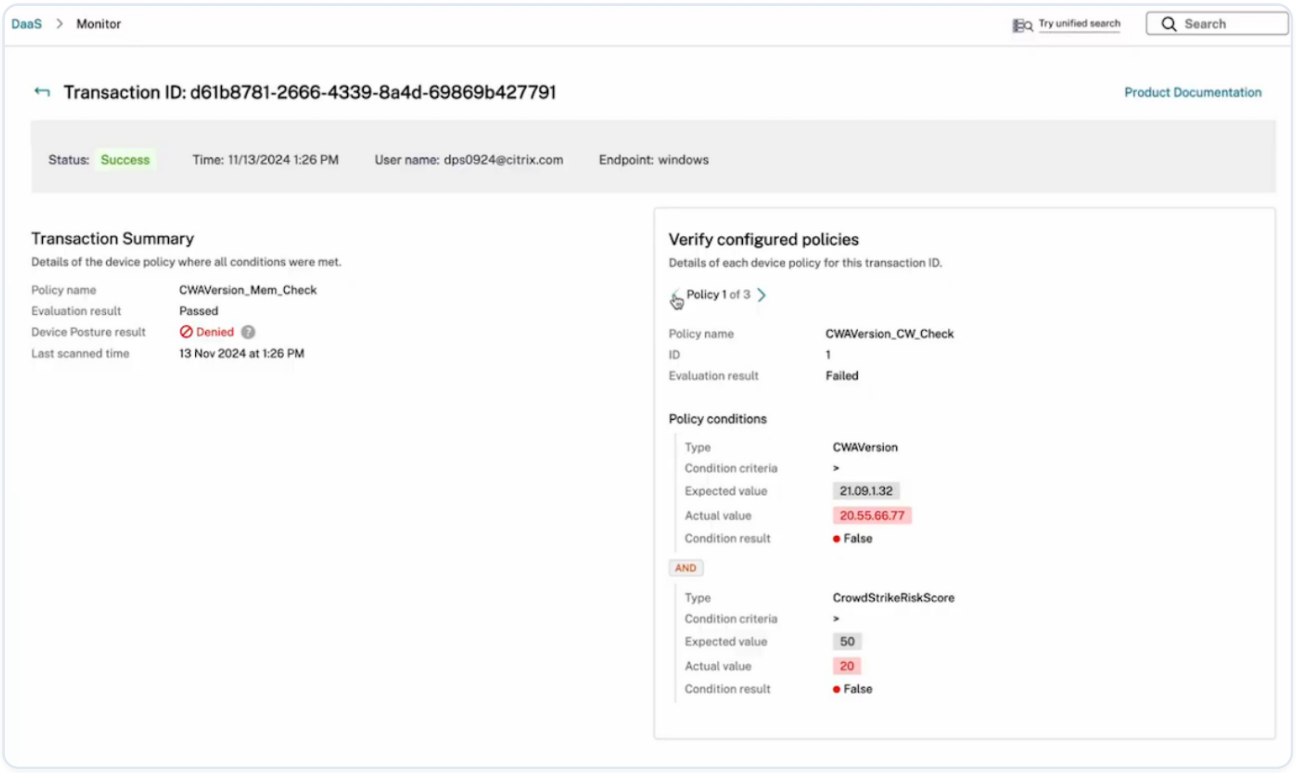


DEBUGGING LARGE POLICY SETS WITH PRECISION SEARCH

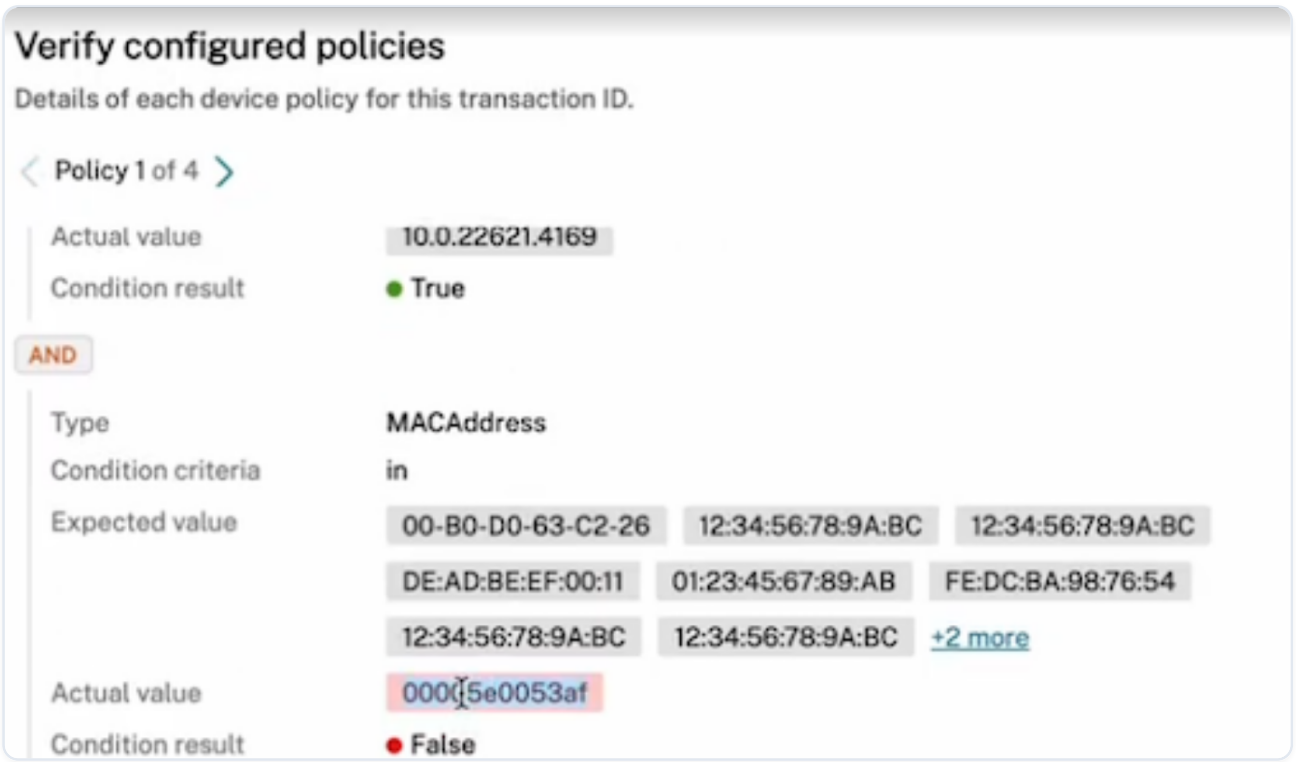
Admins can search for specific parameters in complex environments with multiple policies and verify whether the expected user context is present. The system visually highlights the failing condition if a parameter value mismatch occurs, accelerating root cause identification. Also,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

admins can navigate through policies to see which ones were evaluated and which ones generated the current transaction outcome.



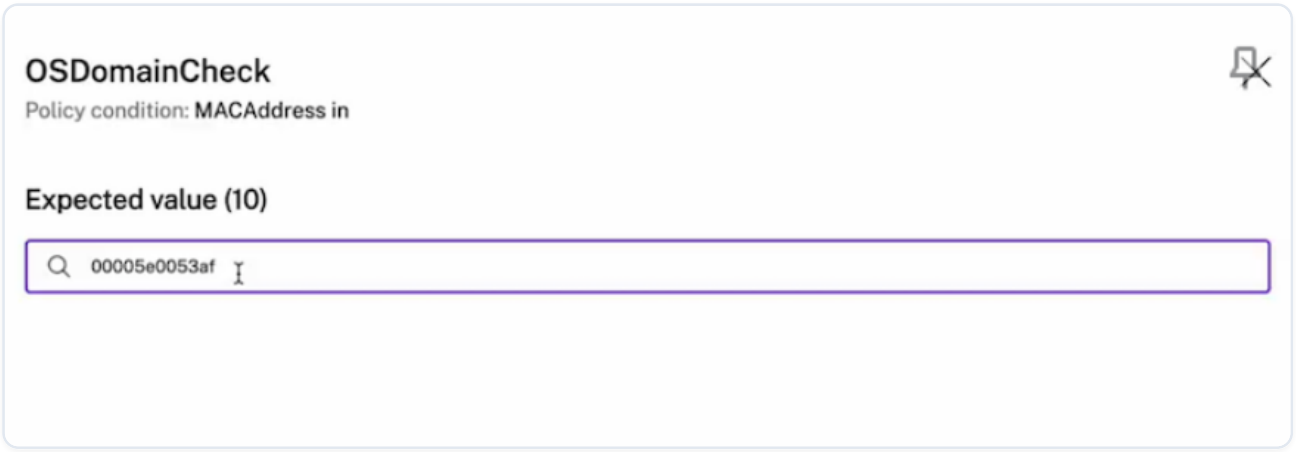
To troubleshoot large working sets of policy parameters, you can search the parameters and see if the desired user context is present in real time.



For example, in the preceding screenshot, the highlighted field, when searched, resulted in no outcome (mentioned in the following image), suggesting that the parameter value did not match.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

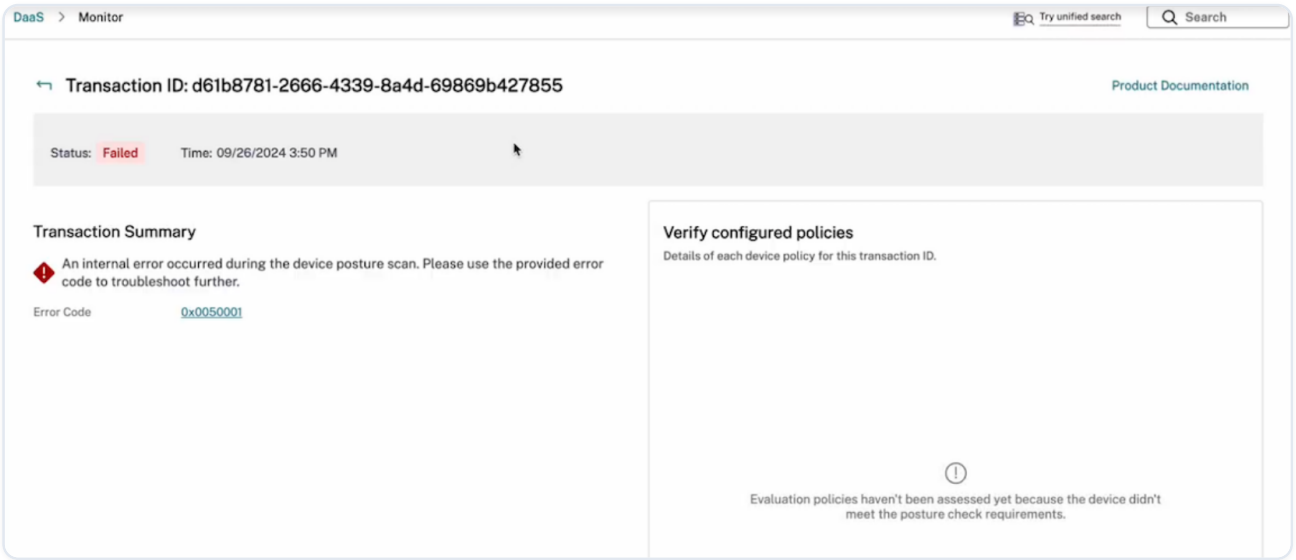
This mismatch caused the condition result to be false and, failing that, the overall policy outcome to be denied.



HANDLING TRANSACTION FAILURES AND ERRORS

If a policy evaluation fails due to a system error, the following details are displayed in Citrix Monitor:

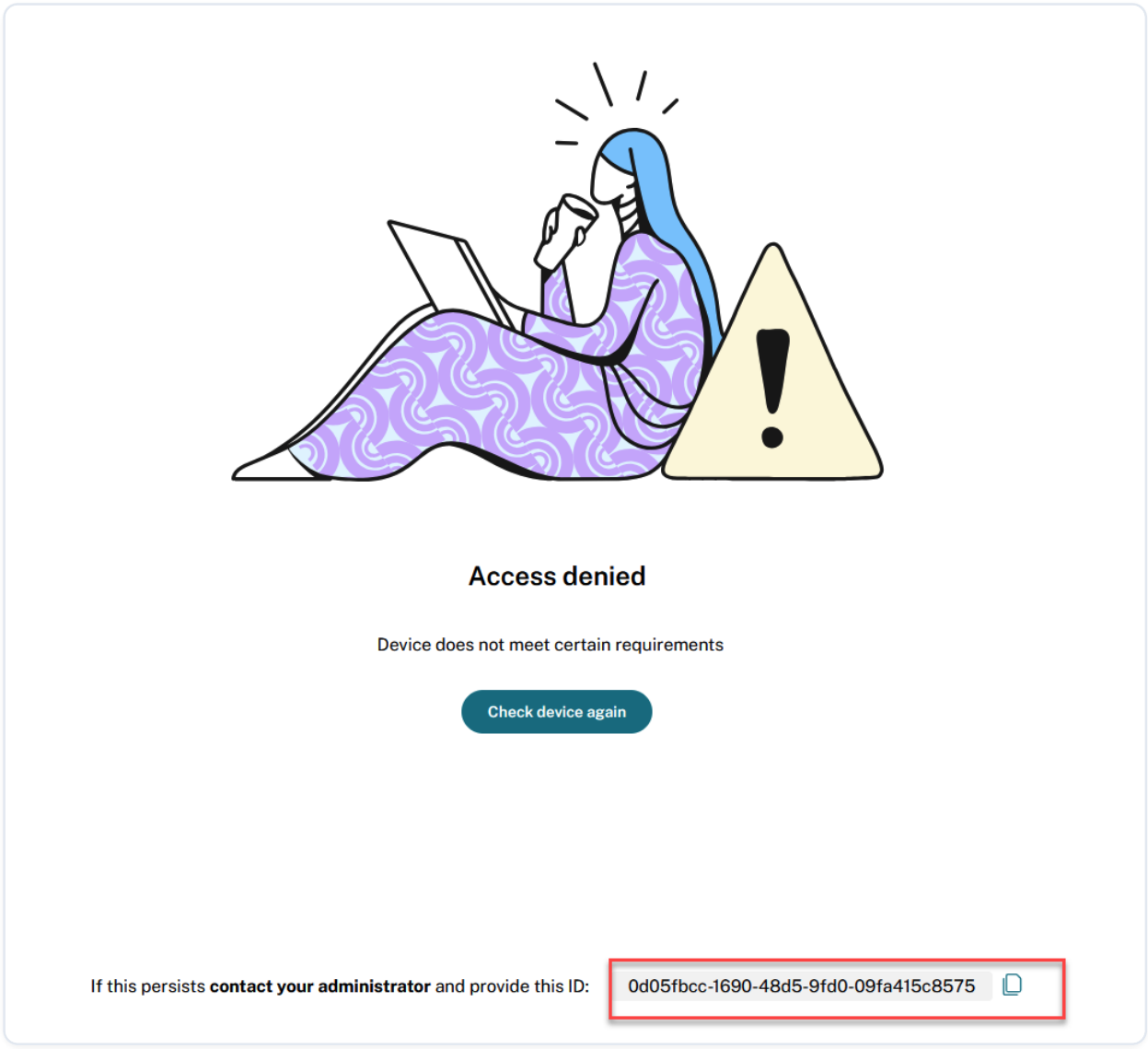
- Error descriptions with contextual details.
- Links to troubleshooting documentation, enabling faster resolution.



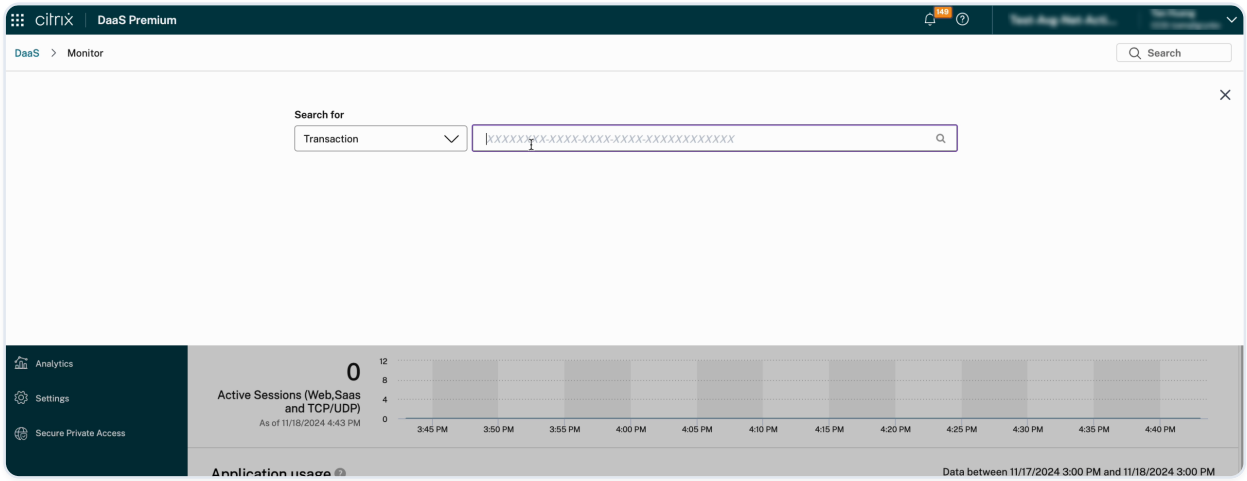
Steps to Diagnose Device Posture Service transactions

1. Copy the transaction ID of the failed or access-denied session from the end-user device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Sign into Citrix Cloud.
3. On the DaaS tile, click **Manage**, and then click the **Monitor** tab.
4. Enter the transaction ID in the **Search** field and click **Details**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can view the transaction summary and the verification details of the configured Device Posture policies. The different values for policy evaluation are compliant, non-compliant, and deny.

TRANSACTION SUMMARY

The **Transaction Summary** page provides the outcome of the Device Posture policy. For compliant, non-compliant, and denied results, the summary includes:

- **Platform**: The OS of the client device.
- **Policy name**: Name of the Device Posture policy.
- **Evaluation result**: Indicates whether the Device Posture policy passed or failed.
- **Device Posture result**: Indicates whether the Device Posture outcome is compliant, non-compliant, or denied.
- **Last scanned time**: The time when the device was last scanned.

VERIFY CONFIGURED POLICIES

The **Verify Configured Policies** section provides comprehensive details of policy evaluation, including:

- Reasons for failure.
- The specific rule that failed.
- Evidence collected.

This information allows admins to troubleshoot and take appropriate actions based on the policy details.
Device posture policy evaluation process

1. **Policy failure and rule identification**:
    - Identify which rule failed and why it failed.
    - Collect evidence related to the failure.
2. **Outcome determination**:
    - Depending on the policy evaluation, the outcome can be compliant, non-compliant, or denied.
    - If no policies match, the outcome is "no matching policy."
3. **Viewing policy details**:
    - Admins can view the details of each device policy for a specific transaction ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Use the backward and forward arrows to navigate through different policies.

In cases of compliant, non-compliant, and denied results, the Device Posture policy evaluation includes the following information in the Verify Configured Policies section:

- **Policy name**: Name of the device policy.
- **ID**: The order in which the policy is evaluated.
- **Evaluation result**: Indicates whether the Device Posture policy passed or failed.
- **Policy result**: Indicates whether the Device Posture outcome is compliant, non-compliant, or denied.
- **Policy Conditions**:
  - **Type**: The device scan type.
  - **Condition criteria**: The condition to evaluate the policy rule.
  - **Expected value**: The configured value of the policy condition.
  - **Actual value**: The evidence collected from the endpoint.
  - **Condition result**: Indicates whether the condition passed or failed.

Error code

When there is an issue and Device Posture fails to evaluate the policy, the error code is displayed.

If there is a failure, copy the error code and contact Citrix support.

The policy details and error codes simplify the triage and troubleshooting of user issues.

The following table provides the error code, error message, and solution for the error:

#	ERROR MESSAGE	ERROR CODE	ACTION
1	Failed to read configured policies.	0x0050001	Contact Citrix Support
2	Failed to evaluate endpoint scans.	0x0050002	Contact Citrix Support
3	Failed to process policies or expression.	0x0050003	Contact Citrix Support

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	ERROR MESSAGE	ERROR CODE	ACTION
4	Failed to save endpoint details.	0x0050004	Contact Citrix Support
5	Failed to process scan results from endpoints.	0x0050005	Contact Citrix Support
6	Failed to read Device Posture mode configuration.	0x0050006	Contact Citrix Support

Diagnose session startup issues

In addition to the logon process phases mentioned in the Diagnose user logon issues section, Monitor displays the session startup duration. This duration is divided into the Workspace App Session Startup duration and the VDA Session Startup duration on the **User Details** and **Endpoint Details** pages. These two durations further contain individual phases whose startup durations are also displayed. This data helps you to understand and troubleshoot high session startup duration. Further, the time duration for each phase involved in the session startup helps in troubleshooting issues associated with individual phases. For example, if the Drive Mapping time is high, you can check to see whether all the valid drives are mapped correctly in the GPO or script.

Prerequisites

Ensure that the following prerequisites are met for session startup duration data to be displayed:

- VDA 1903 or later.
- Citrix End User Experience Monitoring (EUEM) service must be running on the VDA.

Limitations

The following limitations apply when Monitor displays the session startup duration data:

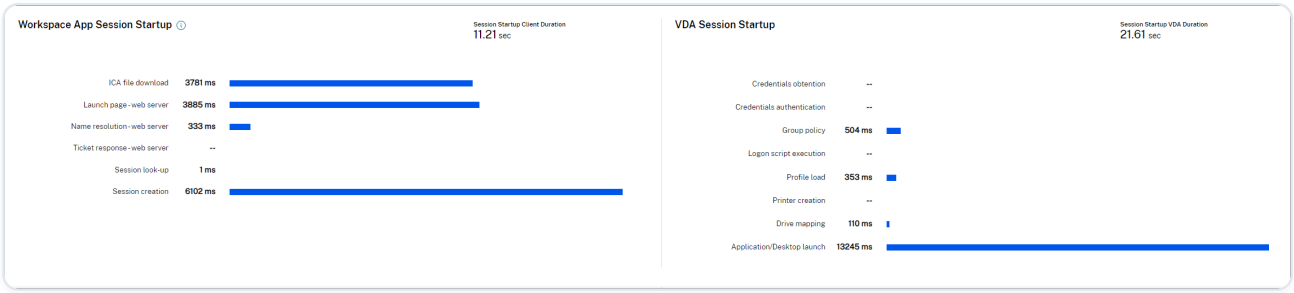
- Session startup duration is available only for HDX™ sessions.
- For session launches from iOS and Android OS, only VDA Startup Duration is available.
- IFDCD is available only when Workspace App is detected while launching from a browser.
- For session launches from macOS, IFDCD is available for Workspace App 1902 and later only.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For session launches from Windows OS, IFDCD is available for Workspace app 1902 and later. For earlier versions, IFDCD is displayed for only app launches from a browser with Workspace app detected.

NOTES:

- If you face issues in the sessions startup duration display after the prerequisites are met, view the Monitor server and VDA logs as described in CTX130320. For shared sessions (multiple applications launched in the same session), the Workspace App Startup metrics are displayed for the latest connection or the latest application launch.
- Some metrics in VDA Session Startup are not applicable on reconnects. In such cases, a message is displayed.



Workspace App session startup phases

SESSION STARTUP CLIENT DURATION (SSCD)

When this metric is high, it indicates a client-side issue that is causing long start times. Review subsequent metrics to determine the probable root cause of the issue. SSCD starts as close as possible to the time of the request (mouse click) and ends when the ICA® connection between the client device and VDA has been established. For a shared session, this duration is much smaller, as much of the setup costs associated with the creation of a new connection to the server are not incurred. At the next level down, there are several detailed metrics available.

ICA FILE DOWNLOAD DURATION (IFDCD)

IFDCD is the time taken for the client to download the ICA file from the server. The overall process is as follows:

1. The user clicks a resource (application or desktop) on the Workspace Application.
2. A request from the user is sent to StoreFront through the Citrix Gateway (if configured), which sends the request to the Delivery Controller.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. The Delivery Controller finds an available machine for the request and sends the machine information and other details to StoreFront. Also, StoreFront requests and receives a one-time ticket from the Secure Ticket Authority.
4. StoreFront generates an ICA File and sends it to the user via Citrix Gateway (if configured).

IFDCD represents the time it takes for the complete process (steps 1–4). The IFDCD duration stops counting when the client receives the ICA file.

LPWD is the StoreFront component of the process.

If IFDCD is high (but LPWD is normal), the server-side processing of the launch was successful, but there were communication issues between the client device and the StoreFront. This results from network issues between the two machines. So you can troubleshoot potential network issues first.

LAUNCH PAGE WEB SERVER DURATION (LPWD)

This is the time taken to process the launch page (launch.aspx) on the StoreFront. If LPWD is high, there might be a bottleneck on the StoreFront.

Possible causes include:

- High load on the StoreFront. Try to identify the cause of slowdown by checking the Internet Information Services (IIS) logs and monitoring tools, Task Manager, Performance Monitor and so on.
- StoreFront is having issues communicating with other components such as Delivery Controller. Check if the network connection between StoreFront and Delivery Controller is slow or some Delivery Controllers are down or overloaded.

NAME RESOLUTION WEB SERVER DURATION (NRWD)

This is the time taken by the Delivery Controller to resolve the name of a published application/ desktop to a VDA Machine IP Address.

When this metric is high, it indicates that the Delivery Controller is taking a long time to resolve the name of a published application to an IP address. Possible causes include:

- a problem on the client
- issues with the Delivery Controller, such as the Delivery Controller being overloaded, or a problem with the network link between them

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TICKET RESPONSE WEB SERVER DURATION (TRWD)

This duration indicates the time it takes to get a ticket (if necessary) from the Secure Ticket Authority (STA) Server or Delivery Controller. When this duration is high, it indicates that the STA server or the Delivery Controller are overloaded.

SESSION LOOK-UP CLIENT DURATION (SLCD)

This duration represents the time taken to query every session to host the requested published application. The check is performed on the client to determine whether an existing session can handle the application launch request. The method used depends on whether the session is new or shared.

SESSION CREATION CLIENT DURATION (SCCD)

This duration represents the time taken to create a session, from the moment wfica32.exe (or a similar equivalent file) is launched to the time when the connection is established.

VDA session startup phases

SESSION STARTUP VDA DURATION (SSVD)

This duration is the high-level server-side connection start-up metric that indicates the time VDA takes to perform the entire start-up operation. When this metric is high, it indicates that there is a VDA issue increasing session start times. This includes the time spent on the VDA performing the entire start-up operation.

CREDENTIALS OBTENTION VDA DURATION (COVD)

The time taken for the VDA to obtain the user credentials.

This duration can be artificially inflated if a user fails to provide credentials in a timely manner, and thus, not included in the VDA Startup Duration. This time is likely to be a significant only if manual login is being used and the server side credentials dialog is displayed (or if a legal notice is displayed before login commences).

CREDENTIALS AUTHENTICATION VDA DURATION (CAVD)

This is the time taken by the VDA to authenticate the user's credentials against the authentication provider, which can be Kerberos, Active Directory, or a Security Support Provider Interface (SSPI).

GROUP POLICY VDA DURATION (GPVD)

This duration is the time taken to apply group policy objects during logon.

LOGIN SCRIPT EXECUTION VDA DURATION (LSVD)

This is the time taken by the VDA to run the user's login scripts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can make the user or group's login scripts asynchronous. Optimize any application compatibility scripts or use environment variables instead.

PROFILE LOAD VDA DURATION (PLVD)

This is the time taken by the VDA to load the user's profile.

If this duration is high, review your User Profile configuration. Roaming profile size and location contribute to slow session starts. When a user logs on to a session where Terminal Services roaming profiles and home folders are enabled, the roaming profile contents and access to that folder are mapped during logon, which takes extra resources. Sometimes, this can consume significant amount of the CPU usage. Use the **Terminal Services home** folders with redirected personal folders to mitigate this problem. In general, use Citrix Profile Management to manage user profiles in Citrix environments. If you are using Citrix Profile Management and have slow logon times, check if your antivirus software is blocking the Citrix Profile Management tool.

PRINTER CREATION VDA DURATION (PCVD)

This is the time taken for the VDA to map the user's client printers synchronously. If the configuration is set for printer creation to be performed asynchronously, no value is recorded for PCVD as it does not impact completion of the session startup.

Excessive time spent in mapping printers is often the result of the printer auto creation policy settings. The number of printers added locally on the users' client devices and your printing configuration can directly affect your session start times. When a session starts, Citrix Virtual Apps and Desktops™ have to create every locally mapped printer on the client device. Reconfigure your printing policies to reduce the number of printers that get created, specifically when users have many local printers. To do this, edit the Printer Auto creation policy in Delivery Controller and Citrix Virtual Apps and Desktops.

DRIVE MAPPING VDA DURATION (DMVD)

This is the time taken by the VDA to map the user's client drives, devices, and ports.

Ensure that your base policies include settings to disable unused virtual channels, such as audio or COM port mapping, to optimize the ICA protocol and improve overall session performance.

APPLICATION/DESKTOP LAUNCH VDA DURATION (ALVD/DLVD)

This phase is a combination of userinit and Shell duration. When a user logs on to a Windows machine, Winlogon runs userinit.exe. Usernit.exe runs logon scripts, re-establishes network connections, and then starts explorer.exe, the Windows User interface. userinit represents the duration between the start of userinit.exe to the start of the user interface for the virtual desktop or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

application. The Shell duration is the time between the initialization of the user interface to the time the user receives keyboard and mouse control.

SESSION CREATION VDA DURATION (SCVD)

This time includes miscellaneous delays in session creation on VDA.

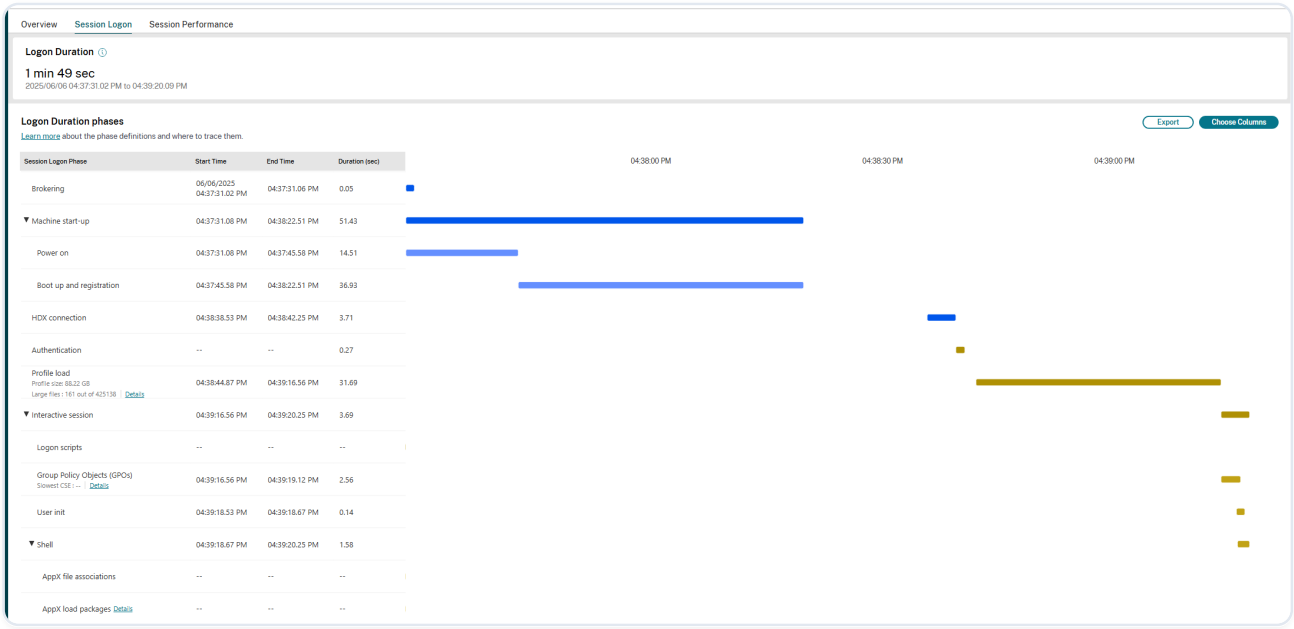
Diagnose user logon issues

The **User Details** view > **Session Logon** tab displays a comprehensive view of the session logon process. You can use Logon Duration data to troubleshoot user logon issues.

Logon duration is measured only for initial connections to a desktop or app using HDX. This data does not include users trying to connect with Remote Desktop Protocol or reconnect from disconnected sessions. Specifically, logon duration is not measured when a user initially connects using a non-HDX protocol and reconnects using HDX.

As users logon to Citrix DaaS™, the Monitor Service tracks the phases of the logon process. The phases begin from the time the user connects from Citrix Workspace™ app to the time when the desktop is ready to use.

The **Session Logon** tab contains the Logon Duration phases chart with the various logon phases plotted. The Logon Duration represents the time spent establishing the connection and obtaining an app or a desktop from Cloud Connector and the time spent to authenticate and log on to a virtual app or desktop. The duration information is presented in seconds (or fractions of seconds).



The Logon Duration phases chart provides a clear view of different logon phases and their start and end times. The chart shows the overlapping of the individual logon phases. The total logon time might not be the sum of the individual logon phase durations. This is because the individual

© 1997–2026 Citrix Systems, Inc. All rights reserved.

phases might overlap and not all logon phases are a part of this representation. Also, certain phases might extend even after the user starts interacting with the virtual app or desktop, and this duration is not measured as part of the overall logon duration.

Use this view to identify specific logon phases causing a delayed session launch. The definition for each logon phase and the event source from where you can trace information helps further troubleshooting. Hovering on the chart gives a tooltip containing the phase duration for the current session as well as the user's 7-day average and the delivery group's 7-day average. This information helps compare the current session logon duration with the 7-day average values. You can further drilldown into subphase measurements in the case of GPO and Profile Details. This visualization helps understand and troubleshoot logon duration-related issues easily

Prerequisites

Ensure that the following prerequisites are met for logon duration data and drilldowns to appear:

1. Install **Citrix User Profile Manager** and **Citrix User Profile Manager WMI Plugin** on the VDA.
2. Ensure that the Citrix Profile Management Service is running.
3. For XenApp and XenDesktop sites 7.15 and earlier, disable the GPO setting, **Do not process the legacy run list**.
4. Audit process tracking must be enabled for Interactive Session drilldown.
5. For GPO drilldown, increase the size of Group Policy operational logs.

NOTE:

Logon duration is supported only on the default Windows shell (explorer.exe) and not on custom shells.

Steps to troubleshoot user logon issues

1. From the **User Details** view, troubleshoot the logon state using the Logon Duration panel.
   - If the user is logging on, the view reflects the process of logging on.
   - If the user is logged on, the Logon Duration panel displays the time it took for the user to log on to the current session.
2. Examine the phases of the logon process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logon process phases

BROKERING

Time taken to decide which desktop to assign to the user.

MACHINE START-UP

If the session required a machine start, this is the time taken to start the virtual machine. The following sub-section provides breakdown of the time taken to start a virtual machine during different phases:

- Power On - Displays the time taken to power on a virtual machine
- Boot-up and registration - Displays the time taken to boot up and register a virtual machine

You can use the collapsible button to collapse or expand the options under the **Machine Start-up**.

HDX CONNECTION

Time taken to complete the steps required in setting up the HDX connection from the client to the virtual machine.

AUTHENTICATION

Time taken to complete authentication to the remote session.

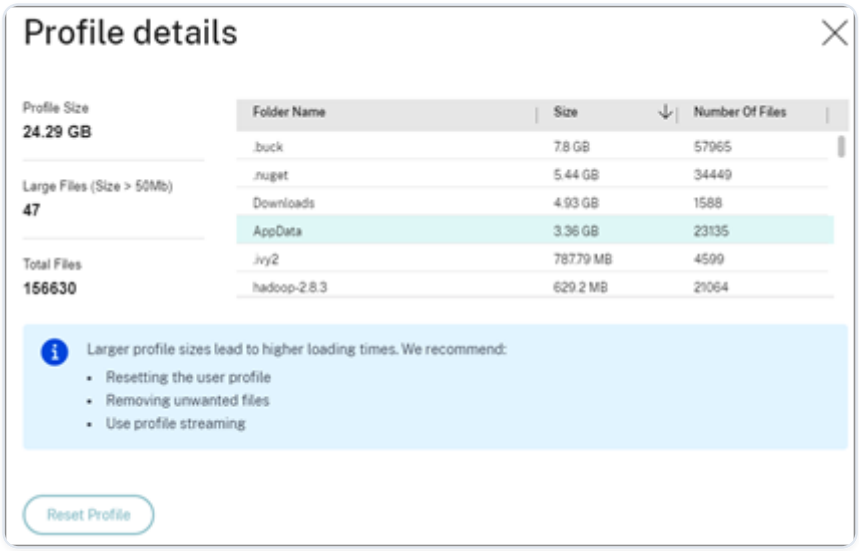
PROFILE LOAD

If profile settings are configured for the user or the virtual machine, this is the time taken for the profile to load.

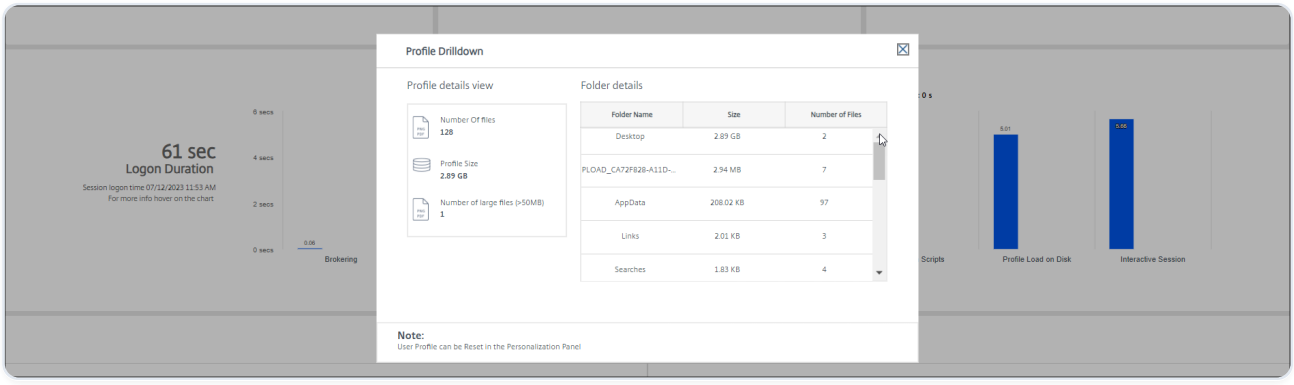
If Citrix Profile Management and FSLogix are configured, the Profile Load bar includes the time taken by Citrix Profile Management and FsLogix to process user profiles. This information helps administrators to troubleshoot high profile processing duration issues. When Profile Management and FSLogix are configured, the Profile Load bar displays an increased duration. This increase is caused by this enhancement and does not reflect a performance degradation. This enhancement is available on VDA versions 2407 or later.

Hovering over the Profile Load bar displays a tooltip showing the user profile details for the current session. This additional information can help troubleshoot high profile load issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Details** to drilldown further into each individual folder in the profile root folder (for instance, C:/Users/username), its size, and the number of files (including files inside nested folders).



Profile drilldown is available on VDAs 1811 and later. Using the profile drilldown information, you can resolve issues involving a high profile load time. You can:

- Reset the user profile
- Optimize the profile by removing unwanted large files
- Reduce the number of files to reduce the network load
- Use profile streaming

By default, all folder names are visible. To hide the folder names, edit the registry values on the VDA machine using the following steps:

WARNING:

Adding and editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix does not guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. On the VDA, add a new registry value **ProfileFoldersNameHidden** at HKEY_LOCAL_MACHINE\Software\Citrix\Director\
2. Set the value to 1. This value must be a DWORD (32-bit) value. Folder names visibility is now disabled.
3. To make the folder names visible again, set the value to 0.

NOTE:

You can use GPO or PowerShell to apply the registry value change on multiple machines. For more information about using GPO to deploy registry changes, see the blog.

Additional information

- Profile drilldown does not consider redirected folders.
- NTUser.dat files in the root folder might not be visible to end users. However, they are included in the profile drilldown and displayed in the list of files in **Root Folder**.
- There are some hidden files in AppData folder which are not included in profile drilldown.
- Number of files and profile size data might not match with the data in the Personalization panel due to certain Windows limitations.

INTERACTIVE SESSION

This is the time taken to "hand off" keyboard and mouse control to the user after the user profile has been loaded. It is normally the longest duration out of all the phases of the logon process and is calculated as **Interactive Session duration = Desktop Ready Event Timestamp (EventId 1000 on VDA) - User Profile Loaded Event Timestamp (EventId 2 on VDA)**. Interactive Session has three subphases: Pre-userinit, Userinit, and Shell. Hover over the Interactive Session to see a tooltip showing the following:

- subphases
- the time taken for each subphase
- the total cumulative time delay between these subphases

You can use the collapsible button to collapse or expand the options under the Interactive Session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

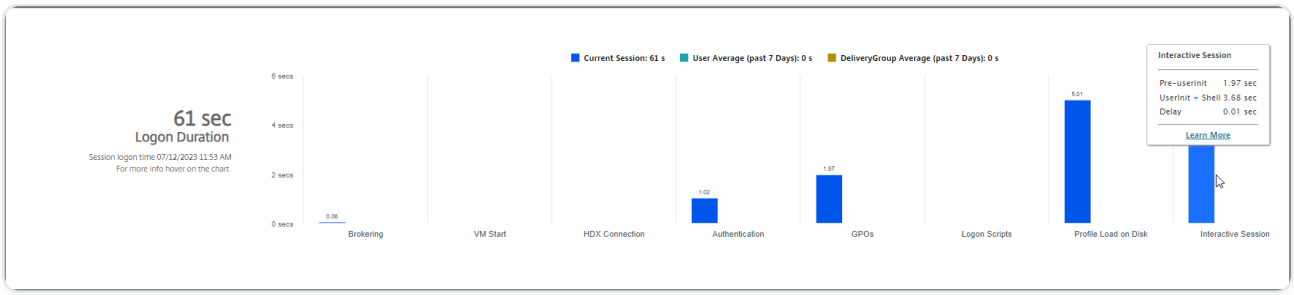
NOTE:

This feature is available on VDAs 1811 and later. If you have launched sessions on sites earlier than 7.18 and then upgraded to 7.18, a ‘Drilldown unavailable due to server error’ message is displayed. However, if you have launched sessions after an upgrade, no error message is displayed.

To view the time duration of each subphase, enable Audit process tracking on the VM (VDA). When the Audit process tracking is disabled (default), the time duration of Pre-userinit and the combined time duration of Userinit and Shell are displayed. You can enable Audit process tracking through a Group Policy Object (GPO) as follows:

1. Create a GPO and edit it using the GPO editor.
2. Go to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy**.
3. On the right pane, double-click **Audit process tracking**.
4. Select **Success** and click OK.
5. Apply this GPO to the required VDAs or Group.

For more information about Audit process tracking and enabling or disabling it, see `<https://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10)>` in the Microsoft documentation.



Logon Duration panel in the User Details view.

- **Interactive Session – Pre-userinit:** This is the segment of Interactive Session which overlaps with Group Policy Objects and scripts. This subphase can be reduced by optimizing the GPOs and scripts.
- **Interactive Session – Userinit:** When a user logs on to a Windows machine, Winlogon runs userinit.exe. Userinit.exe runs logon scripts, re-establishes network connections, and then starts Explorer.exe, the Windows user interface. This subphase of Interactive Session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

represents the duration between the start of Userinit.exe to the start of the user interface for the virtual desktop or application.

- **Interactive Session – Shell:** In the previous phase, Userinit starts the initialization of Windows user interface. The Shell subphase captures the duration between the initialization of the user interface to the time user receives keyboard and mouse control.
- **Delay:** This is the cumulative time delay between the **Pre-userinit and Userinit** subphases and the **Userinit and Shell** subphases.

The total logon time is not an exact sum of these phases. For example, some phases occur in parallel, and in some phases, extra processing occurs that can result in a longer logon duration than the sum. The total logon time does not include the ICA® idle time that is the time between the ICA file download and the ICA file launch for an application. To enable the automatic opening of ICA file upon application launch, configure your browser for automatic ICA file launch upon download of an ICA file. For more information, see CTX804493.

NOTE:

The Logon Duration graph shows the logon phases in seconds. Any duration values below one second are displayed as subsecond values. The values above one second are rounded to the nearest 0.5 second. The graph has been designed to show the highest y-axis value as 200 seconds. Any value greater than 200 seconds is shown with the actual value displayed above the bar.

Logon scripts
If logon scripts are configured for the session, this is the time taken for the logon scripts to be run.
GPOs
If Group Policy settings are enabled on the virtual machines, this is the time taken to apply group policy objects during logon. The drill-down of the time taken to apply each policy as per the CSEs (Clients-Side Extension) is available as a tooltip when you hover on the GPO bar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Details** to see a table with the policy status, and the corresponding GPO name. The time durations in the drilldown represent the CSE processing time only and do not add up to the total GPO time. You can copy the drill-down table for further troubleshooting or use in reports. The GPO time for the policies is retrieved from Event Viewer logs. The logs can get overwritten depending on the memory allocated for the operational logs (default size is 4 MB). For more information about increasing the log size for the operational logs, see the Microsoft TechNet article Configuring the Event Logs.

User init

When a user logs on to a Windows machine, Winlogon runs userinit.exe. Userinit.exe runs logon scripts, re-establishes network connections, and then starts Explorer.exe, the Windows user interface. This subphase of Interactive Session represents the duration between the start of Userinit.exe to the start of the user interface for the virtual desktop or application

SHELL

The Shell subphase captures the duration between the initialization of the user interface to the time the user receives keyboard and mouse control.

AppX file associations

The time taken to associate AppX files during the new VDA session.

AppX load packages

The time taken to load the AppX packages during the new VDA session.

NOTE:

uberAgent must be integrated with Monitor for collecting AppX packages loading duration during the new VDA session. For this integration, install VDA and then configure uberAgent via Citrix policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EXPORT DATA

Along with the default Logon Duration Phases table options, which is Session Logon Phase and Duration, you can also choose the following columns on the Session Logon page:

- Start time
- End time
- Delivery Group - 7d Avg (sec)
- User - 7d Avg (sec)

You can also export the preceding data to a .CSV file.

Troubleshooting tips

To identify unusual or unexpected values in the graph, compare the amount of time taken in each phase of the current session with the average duration for this user for the last seven days, and the average duration for all users in this delivery group for the last seven days.

Escalate as needed. For example, if the **Machine Start-up** is slow, the issue might be in the hypervisor, so you can escalate it to the hypervisor administrator. Or, if the brokering time is slow, you can escalate the issue to the site administrator to check the load balancing on the Delivery Controller.

Examine unusual differences, including:

- Missing (current) logon bars
- Major discrepancy between the current duration and this user's average duration. Causes include:
  - A new application was installed.
  - An operating system update occurred.
  - Configuration changes were made.
  - Profile size of the user is high. In this case, the Profile Load is high.
- Major discrepancy between the user's log on numbers (current and average duration) and the delivery group average duration.

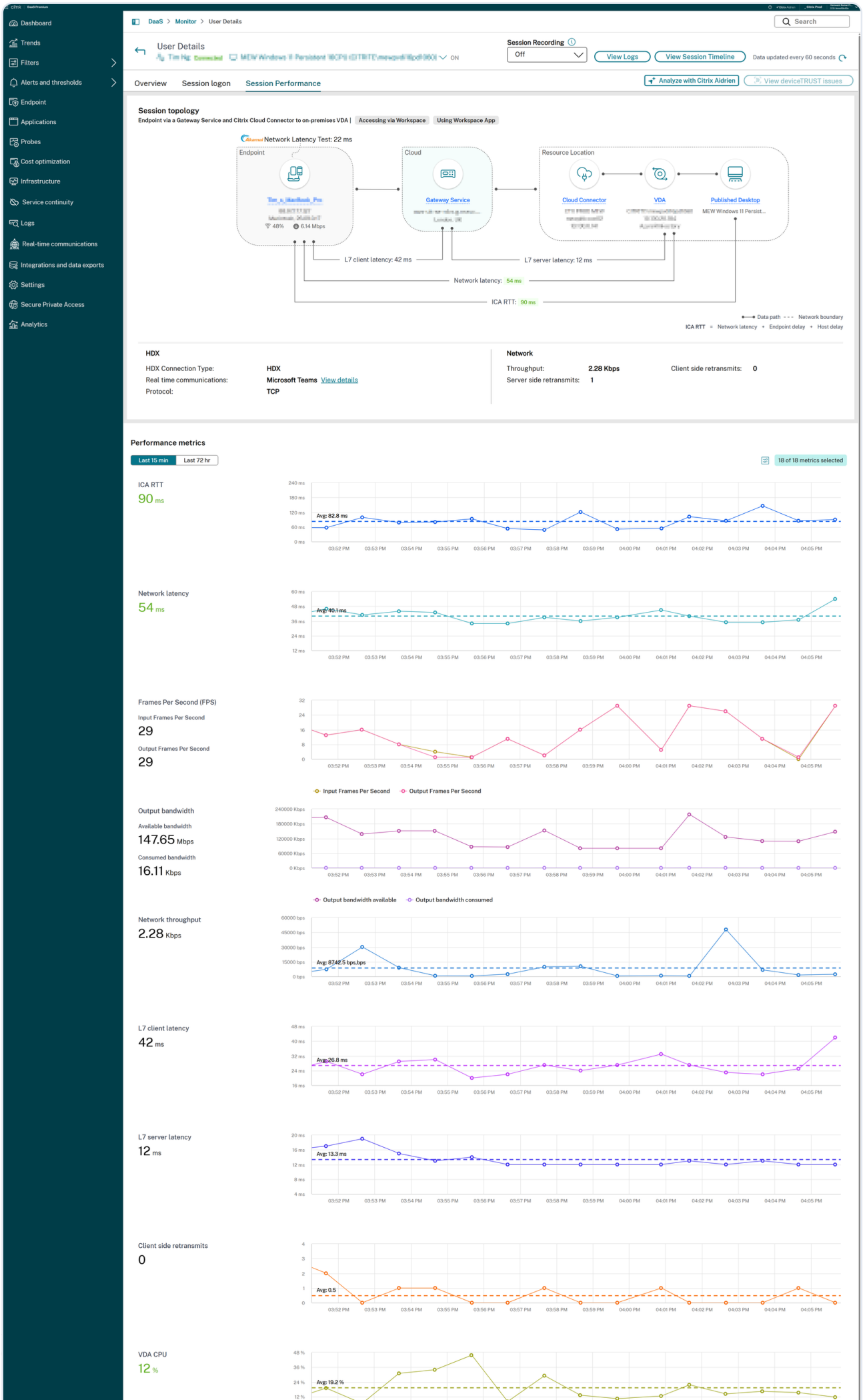
If needed, click **Restart** to observe the user’s logon process to troubleshoot issues, such as Machine Start-up or Brokering.

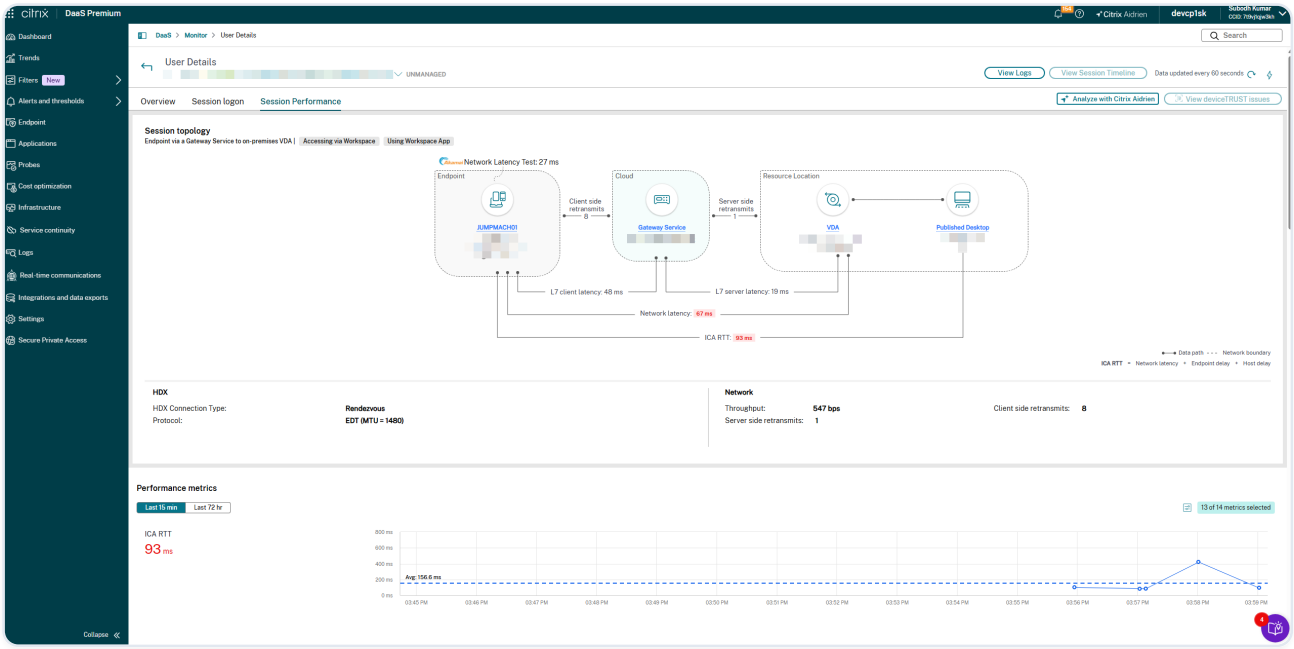
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diagnose session performance issues

The **Session Performance** tab on the User Details Page has enhanced troubleshooting workflows to help identify issues within HDX™ user sessions. The **Session Topology and Performance Metrics** panels help correlate the component view and multiple performance metrics of a session in a single view and reduces the mean time for resolution of session experience issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Dashboard
Trends
Filters
Alerts and thresholds
Endpoint
Applications
Probes
Cost optimization
Infrastructure
Service continuity
Logs
Real-time communications
Integrations and data exports
Settings
Secure Private Access
Analytics
DaaS > Monitor > User Details
Search
User Details
Session Recording
Off
View Logs
View Session Timeline
Data updated every 60 seconds
Overview
Session logon
Session Performance
Analyze with Citrix Aidrien
View deviceTRUST issues
Session topology
Endpoint via a Gateway Service and Citrix Cloud Connector to on-premises VDA |
Accessing via Workspace
Using Workspace App
Network Latency Test: 22 ms
Endpoint
Cloud
Resource Location
Gateway Service
Cloud Connector
VDA
Published Desktop
MEW Windows 11 Persist...
6.14 Mbps
L7 client latency: 42 ms
L7 server latency: 12 ms
Network latency: 54 ms
ICA RTT: 90 ms
Data path
Network boundary
ICA RTT = Network latency + Endpoint delay + Host delay
HDX
HDX Connection Type: HDX
Real time communications: Microsoft Teams View details
Protocol: TCP
Network
Throughput: 2.28 Kbps
Server side retransmits: 1
Client side retransmits: 0
Performance metrics
Last 15 min
Last 72 hr
18 of 18 metrics selected
ICA RTT
90 ms
Avg: 82.8 ms
Network latency
54 ms
Avg: 40.1 ms
Frames Per Second (FPS)
Input Frames Per Second
29
Output Frames Per Second
29
Input Frames Per Second
Output Frames Per Second
Output bandwidth
Available bandwidth
147.65 Mbps
Consumed bandwidth
16.11 Kbps
Output bandwidth available
Output bandwidth consumed
Network throughput
2.28 Kbps
Avg: 8742.5 bps,bps
L7 client latency
42 ms
Avg: 26.8 ms
L7 server latency
12 ms
Avg: 13.3 ms
Client side retransmits
0
Avg: 0.5
VDA CPU
12 %
Avg: 19.2 %



End-to-end Network Hop view

The end-to-end network hop view offers a visual representation of the complete session path, significantly aiding in troubleshooting. You can access this view from **User Details** > **Session Performance** > **Session Topology**. The end-to-end network hop view displays components, metadata, links, and published applications for connected HDX sessions.

This view helps administrators to:

- Understand session data flow.
- Identify performance bottlenecks at specific hops.

SESSION PERFORMANCE METRICS

The following metrics are available contextually to help administrators understand the performance of the given session. The metrics presented in the end-to-end network hop view are available in near real-time and refresh periodically based on the intervals shown in the UI.

Endpoint metrics

Endpoint metrics are vital for troubleshooting Citrix® session performance as they provide insights into the "last mile" of the user experience and reveal details about the user's immediate environment. These metrics help identify local bottlenecks, such as poor Wi-Fi, low network throughput, endpoint device limitations, distinguishing between server-side and client-side problems. By offering a holistic view when combined with metrics in the session topology, endpoint data enables faster root cause identification and quicker resolution of performance issues, improving the user experience.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use the policies in Citrix Studio to enable or disable collection of listed endpoint metrics based on your requirements. The policies provide Citrix administrators granular controls to report metrics in adherence to your compliance requirements.

POLICY NAME	POLICY DESCRIPTION	UI METRICS	DEFAULT VALUE	VALUE OPTIONS	VDA WINDOWS VERSION	VDA MAC VERSION	VDA LINUX VERSION
Endpoint statistics interval	Allows the collection of endpoint network details from the user endpoint. Enabling this policy is a pre-requisite for other endpoint related policies to take effect.	Wi-Fi signal strength, Network interface type, Throughput incoming or outgoing, Link speed, Workspace type, Endpoint CPU, Endpoint memory, Endpoint GPU	Enabled	Enabled or Disabled. Option to modify the frequency between 60s - 3600s. 60s is suggested value	2407 or later	2607	2607
Endpoint location data collection	Allows the collection of endpoint location	Public IP address, Country, City, and	Disabled	Enabled or Disabled	2411 or later	2607	2607

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLICY NAME	POLICY DESCRIPTION	UI METRICS	DEFAULT VALUE	VALUE OPTIONS	VDA WINDOWS VERSION	VDA MAC VERSION	VDA LINUX VERSION
	and ISP details from the user endpoint using the Locus service - https://locus.analytics.cloud.com	Internet Service Provider.					
Endpoint network latency measurement interval	Allows the measurement and collection of network latency between the endpoint and the beacon host - https://downloadplugins.citrix.com	Network latency (under Endpoint network details)	Disabled	Enabled or Disabled. Option to modify the frequency between 60s - 3600s. 60s is suggested value	2411 or later	2607	2607

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

From Citrix Virtual Apps and Desktops™ 2507 or later, **Endpoint location data collection** policy and **Endpoint network latency measurement interval** policy are disabled by default. Consequently, the related data is unavailable in Director unless these policies are manually enabled in Studio.

Endpoint metrics that are readily available are listed below:

- Endpoint name
- Endpoint IP
- Endpoint OS
- Citrix Workspace™ app version

The following table lists metrics dependent on supported product versions:

FEATURE NAME	UI PARAMETERS	VDA WINDOWS VERSION	VDA MAC VERSION	VDA LINUX VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROME OS VERSION
Endpoint network details	Network interface type	2407 or later	NA	NA	2405.10 or later	2409 or later	2408 or later	2411 or later	2411 or later
	Signal strength	2407 or later	NA	NA	2405.10 or later	2409 or later	2408 or later	Not applicable	Not applicable

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	VDA WINDOWS VERSION	VDA MAC VERSION	VDA LINUX VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROME OS VERSION
	Endpoint throughput (incoming, outgoing)	2407 or later	NA	NA	2405.10 or later	2409 or later	2408 or later	Not applicable	Not applicable
	Link speed	2407 or later	NA	NA	2405.10 or later	2409 or later	2408 or later	2411 or later	2411 or later
	Endpoint public IP address	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	2411 or later	2411 or later
	Endpoint City, Endpoint country	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	2411 or later	2411 or later
	Internet servi	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	2411 or later	2411 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	VDA WINDOWS VERSION	VDA MAC VERSION	VDA LINUX VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROME OS VERSION
	ce provider								
	Workspace type	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	2411 or later	2411 or later
	Access type (via Workspace / StoreFront)	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	2411 or later	2411 or later
	Endpoint CPU	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	Not applicable	2411 or later
	Endpoint memory	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	Not applicable	2411 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	VDA WINDOWS VERSION	VDA MAC VERSION	VDA LINUX VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROME OS VERSION
	Endpoint GPU	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	Not applicable	Not applicable
	Network latency	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	2411 or later	2411 or later

Data definitions:

UI PARAMETER	DESCRIPTION
Endpoint name	Name of the user's endpoint device used for the session.
Endpoint IP	IP address of the endpoint as available to the Virtual Delivery Agent (VDA). It might contain private or public IP addresses of the endpoint device.
Endpoint OS	Operating system of the endpoint device
Citrix Workspace App version	Installed Citrix Workspace app version
Signal strength	Displays the quality and strength of the wireless signal.
Endpoint throughput (incoming, outgoing)	Indicates the rate of data transfer into and out of the network interface. Analogous to the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UI PARAMETER	DESCRIPTION
	upload and download internet speed observed on the endpoint.
Link speed	Specifies the type of network connection, such as Ethernet, Wi-Fi, or cellular.
Network interface type	Represents the maximum data transfer rate of the network connection.
Endpoint public IP address	The external IP address assigned to your device by your internet service provider.
Endpoint City, Endpoint country	The geographical location, including country and city, of the device.
Internet service provider	The name of the company that provides internet access to the end user device.
Workspace type	The type of workspace being used, either Citrix Workspace app or a web browser.
Access type (via Workspace / StoreFront)	The method of accessing resources, either through Citrix® StoreFront Cloud (formerly known as Citrix Workspace) or on-premises StoreFront.
Endpoint CPU	The percentage of CPU resources currently being used.
Endpoint memory	The percentage of memory resources currently being used.
Endpoint GPU	The percentage of GPU resources currently being used.
Network latency test	The time delay experienced in the network, measured in milliseconds.

Network metrics

Network metrics are critical for Citrix session troubleshooting because the performance and stability of a Citrix session are heavily dependent on the underlying network conditions. Unlike a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

local application, a Citrix session involves streaming an interactive desktop or application experience over a network, meaning any network instability or bottleneck will directly impact the user's perception of performance.

Collection of network metrics can be enabled or disabled via Citrix policies in Citrix Studio. For additional information on requirements for network metrics, see Network telemetry.

SETTING NAME	POLICY DESCRIPTION	UI METRICS	DEFAULT VALUE	VALUE OPTIONS	VIRTUAL DELIVERY AGENT VERSION
Network telemetry	Allows the collection of network details between the user endpoint and the backend components.	All HDX insights metrics for Citrix Gateway and Citrix Gateway service	Disabled	Enabled or Disabled.	2411 or later for Gateway service. 2503 or later for Citrix Gateway

Citrix Gateway Service

The following table lists metrics dependent on supported product versions:

FEATURE NAME	UI PARAMETERS	WINDOWS VDA VERSION	MAC VDA VERSION	LINUX VDA VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROMEOS VERSION
Network	L7 Server	2411 or	2507 or later	2507 or later	2409 or later	2505 or later	2505 or later	2607	2607

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	WINDOWS VDA VERSION	MAC VDA VERSION	LINUX VDA VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROME OS VERSION
metrics	latency	above							
	L7 Client latency	2411 or above	2507 or later	2507 or later	2409 or later	2505 or later	2505 or later	2607	2607
	Client Side Retransmits Note: Available only for TCP sessions	2411 or above	2507 or later	2507 or later	2409 or later	2505 or later	2505 or later	2607	2607
	Throughput	2411 or above	NA	NA	2409 or later	2505 or later	2505 or later	2607	2607

Citrix Gateway

The following table lists metrics dependent on supported product versions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	CITRIX GATEWAY VERSION	WINDOWS VDA VERSION	MAC VERSION	LINUX VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROMEOS VERSION
Network metrics	WAN latency	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607
	DC latency	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607
	Server Side Retransmits	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	CITRIX GATEWAY VERSION	WINDOWS VDA VERSION	MAC VERSION	LINUX VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROMEOS VERSION
	Client Side Retransmits	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607
	L7 server latency	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607
	L7 Client latency	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	CITRIX GATEWAY VERSION	WINDOWS VDA VERSION	MAC VERSION	LINUX VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROMEOS VERSION
	Client side Zero Window size event	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607
	Client side fast RTO	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607
	Server side Zero Window size event	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	CITRIX GATEWAY VERSION	WINDOWS VDA VERSION	MAC VERSION	LINUX VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROMEOS VERSION
	Server side fast RTO	Netscaler 14.1-47.46 or above	2503 or later	2507 or later	2507 or later	2503 or later	2505 or later	2505 or later	2607	2607

Data definitions:

UI PARAMETER	DESCRIPTION
WAN latency	Latency caused by the client side of the network, from NetScaler® to the end user.
DC latency	Latency caused by the server side of the network, from NetScaler to backend servers.
L7 Client latency	The average L7 latency observed between the ICA® client and the NetScaler instance. This metric is useful in non-Citrix devices that are present in the delivery path.
L7 Server latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UI PARAMETER	DESCRIPTION
	This metric is useful when non-Citrix devices are present in the delivery path.
Client retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric indicates high bandwidth utilization due to retransmits but does not necessarily mean a poor user experience. Note: For sessions using Gateway service, Client retransmits are only available for TCP sessions.
Server side retransmits	The number of packets retransmitted on the connection between NetScaler and the back-end server.
Client side zero window count	The number of times the client advertised a zero TCP window.
Server side zero window count	The number of times the server advertised a zero TCP window.

HDX metrics

HDX metrics are fundamental to understanding and troubleshooting the quality of the user's virtual experience. These metrics directly measure the performance of the ICA/HDX protocol that delivers the virtual session.

NOTE:

ICA metrics are available starting with Citrix Workspace app for Windows version 2405.10 or later, and Citrix Virtual Apps and Desktops 2407 or later. However, updates and fixes to the data are available in recent versions. Refer to the following table for the recommended versions for each data point:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	WINDOWS VDA VERSION	MAC VDA VERSION	LINUX VDA VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION
ICA metrics	ICA RTT	2507 or later	NA	NA	2503 or later	2503 or later	2503 or later	2503 or later
	Network latency	2507 or later	NA	NA	2503 or later	2503 or later	2503 or later	2503 or later
	HDX connection type	2411 or later	NA	NA	2411 or later	2411 or later	2411 or later	2411 or later
	Protocol	2411 or later	NA	NA	2411 or later	2411 or later	2411 or later	2411 or later
	EDT MTU	2411 or later	NA	NA	2411 or later	2411 or later	2411 or later	2411 or later

Data definitions:

UI PARAMETER	DESCRIPTION
ICA RTT	Measures the time between user action and screen response. Thinwire RTT counter represents this metric starting with Citrix Virtual Apps and Desktops version 2507. Previous versions continue to use the EUEM RTT.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UI PARAMETER	DESCRIPTION
Network latency	Indicates network latency and potential slowness. Defined as the sum of client and server side latency starting with Citrix Virtual Apps and Desktops version 2503. Previous versions continue to use HDX latency reported on the VDA.
HDX Connection type	Type of HDX connection for the user session.
Protocol	Underlying protocol used for the user session. Values can be *TCP* or *EDT*.
EDT MTU	MTU, referred to as Maximum Transmission Unit, is the largest size of a packet (in bytes) that a network interface can send without needing to fragment it. EDT MTU represents the MTU established for the EDT session of the user.

Real-time communications optimization visibility

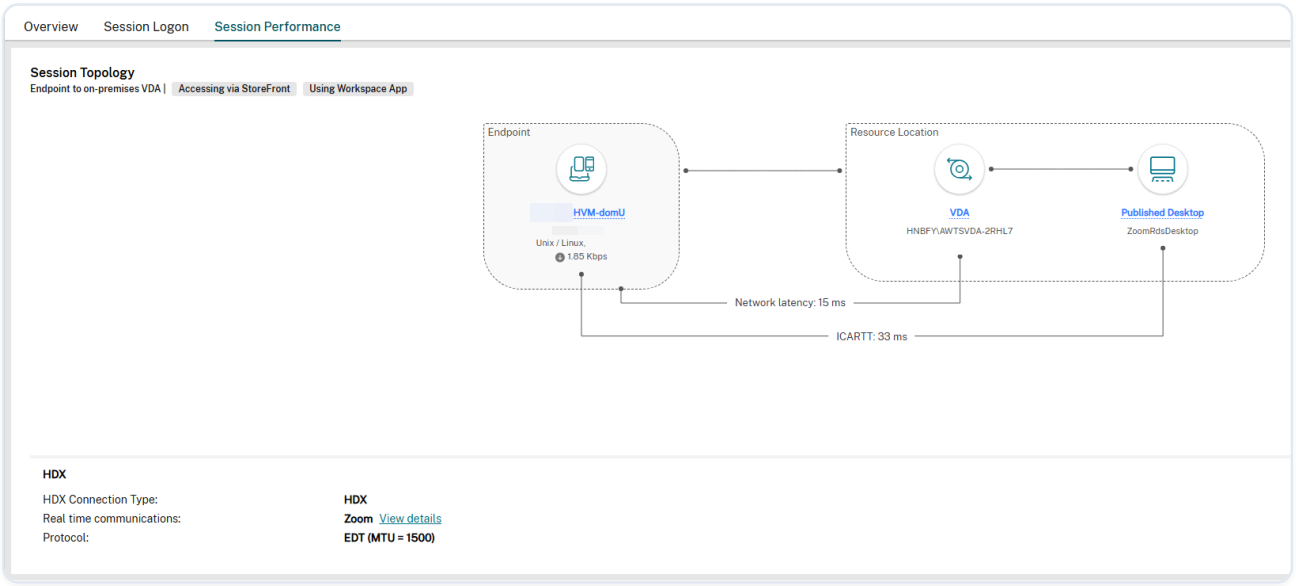
The session topology provides comprehensive visibility into the optimization status of real-time communication (RTC) applications like Microsoft Teams, Zoom, and WebEx within Citrix sessions. It pinpoints whether an application is optimized, and identifies any missing components (such as necessary plugins, plugin management, or platform-specific limitations) that prevent optimal performance.

Benefits:

- Customers get clear assurance regarding RTC application optimization, eliminating guesswork about whether a session is truly optimized.
- Direct insight into missing components to proactively address issues and achieve full optimization.
- Faster troubleshooting improves the user experience for important communication tools.

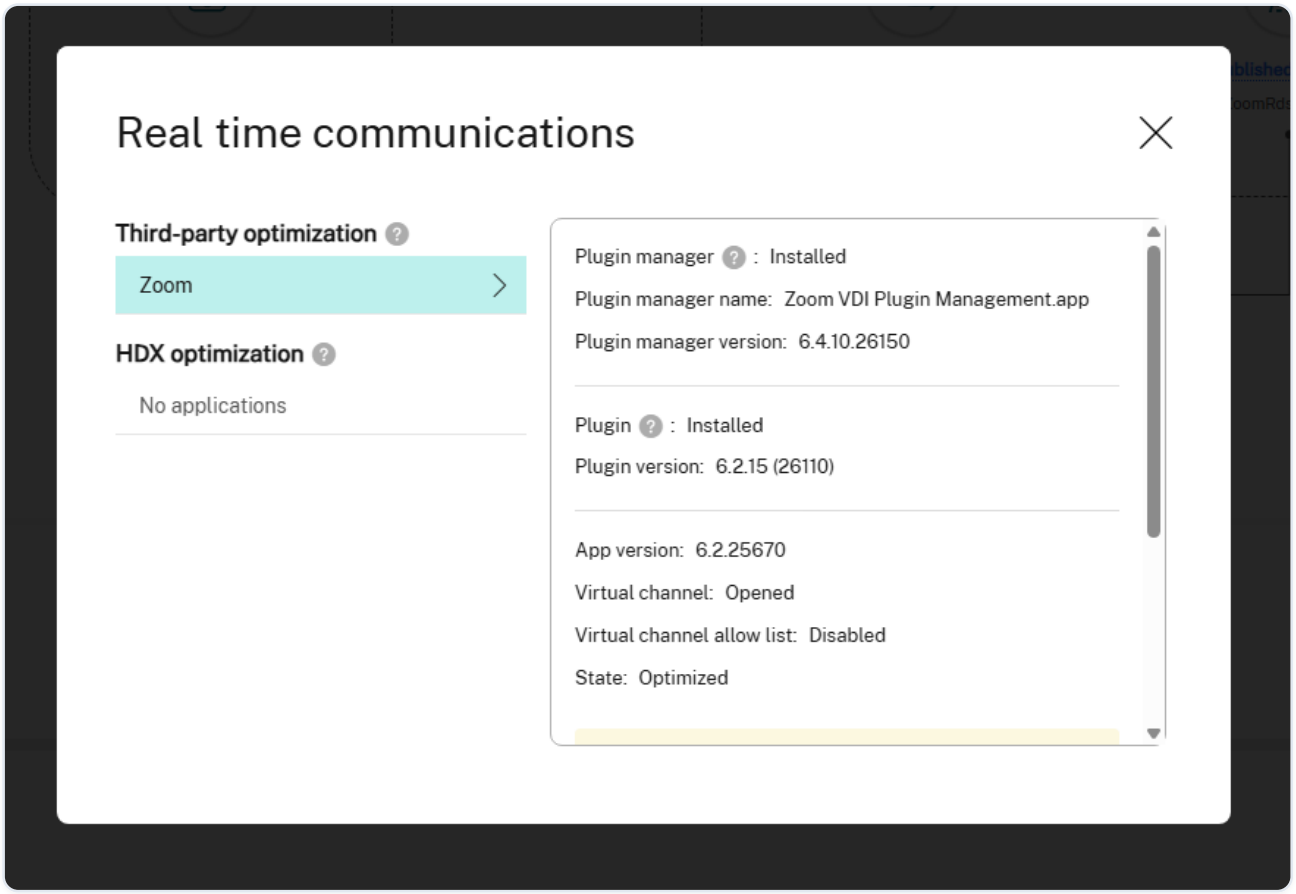
Use the **Real time communications** field in the **Session Topology** to view optimization details for each application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Third-party optimized applications create a virtual channel using Citrix technology, but the application vendor manages other configurations and settings. The optimization relies on solutions owned by the vendor.

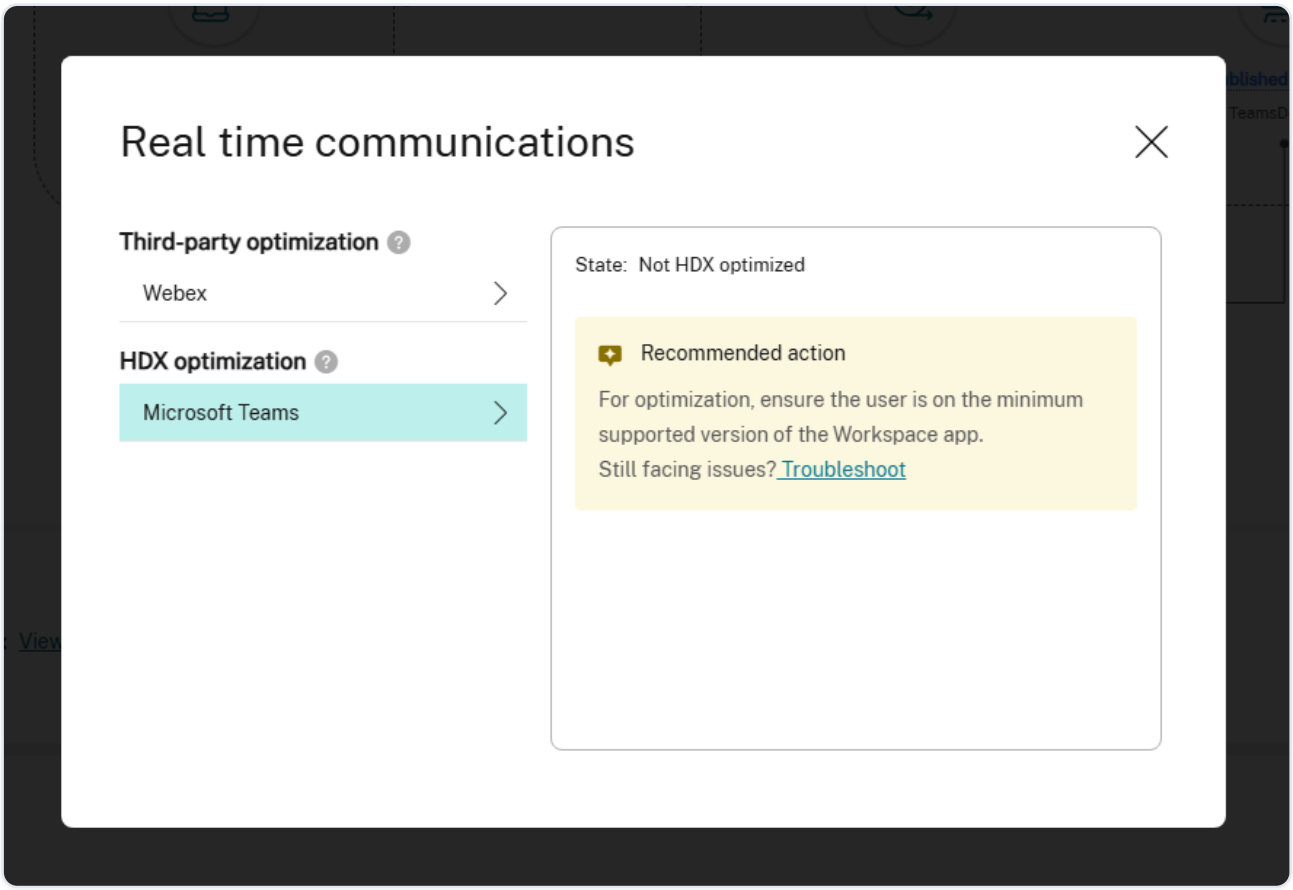
Click the **View details** link next to the **Real time communications** field in the **Session Topology** screen. The following screen appears:



HDX-optimized applications use the Citrix virtual channel and are directly impacted by Citrix configurations and settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click the **HDX optimization** section on the **Real time communications** screen. The following image appears:



The real time communications details are updated every 5 minutes. The following table lists available details for an application that relies on third-party optimization. Ensure you are using supported product versions to get full visibility.

Note:

- Microsoft Teams Slimcore Optimization is available only for published desktops and for New Teams as per vendor support.
- For Zoom, the vendor changes to fetch plug-in details and optimization states are available from version 6.3.10 onwards. For more information, see Zoom documentation.

The following table lists available details for an application that relies on Citrix HDX optimization. Ensure that you are using supported product versions to get full visibility.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	VIRTUAL DELIVERY AGENT VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION
Microsoft Teams Slimcore	Plugin manager, Plugin manager name, Plugin manager version	2503	2503	Not supported by vendor	Not supported by vendor
	App version, Virtual channel, Virtual channel allow list	2503	2402	Not supported by vendor	Not supported by vendor
	Plugin, Plugin version, State	2507	2503	Not supported by vendor	Not supported by vendor
Zoom	Plugin manager, Plugin manager name, Plugin manager version	2507	2503	2505	Plugin not Available
	App version, Virtual channel, Virtual channel allow list	2507	2402	2402	2402

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE NAME	UI PARAMETERS	VIRTUAL DELIVERY AGENT VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION
	Plugin, Plugin version, State	2507	2503	2505	Plugin Not Available
Webex	Plugin manager, Plugin manager name, Plugin manager version	2507	2503	Plugin Not Available	Plugin Not Available
	App version, Virtual channel, Virtual channel allow list	2507	2402	2402	2402

The following table lists available details for an application that relies on Citrix HDX optimization. Ensure that you are using supported product versions to get full visibility.

FEATURE NAME	UI PARAMETERS	VIRTUAL DELIVERY AGENT VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION
Microsoft Teams	State	1906.2	2112	2203	2203

Data definitions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UI PARAMETER	DESCRIPTION
Plugin manager	Shows whether the plugin manager is installed or not. The plug-in manager is a small management component that opens the Virtual channel and downloads the necessary media engine (plugin) for optimization. Note: Functionality might vary by vendor.
Plugin manager name	Name of the installed plugin manager.
Plugin manager version	Version of the installed plugin manager.
Plugin	Shows whether the plugin is installed or not. Plugin is the necessary media engine for optimization. Note: Functionality might vary by vendor.
Plugin version	Version of the installed plugin on the endpoint.
App version	Represents the version of the application on the virtual delivery agent (VDA).
Virtual channel	Represents if the virtual channel is open or closed for the real time communications app.
Virtual channel allow list	Shows the status of virtual channels. Values are *Enabled* or *Disabled*.
State	Shows the optimization state for the application for the specific user session

SESSION TOPOLOGY SCENARIOS

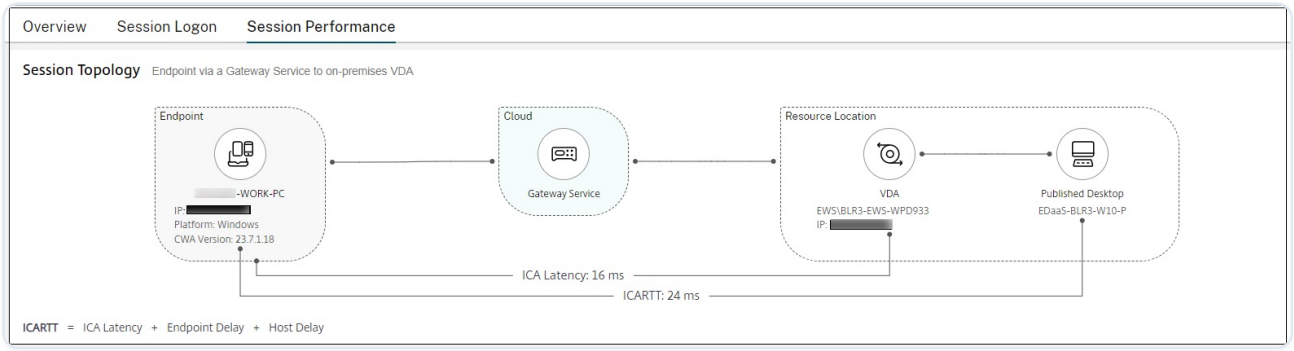
Depending on the deployment scenario of the site, the components involved in a session are all or any of the following:

- Citrix Workspace app on Endpoint
- Gateway service/ on-premises Gateway
- Cloud Connector – Gateway is connected to DaaS via a Cloud Connector in the case of hybrid connections.
- VDAs

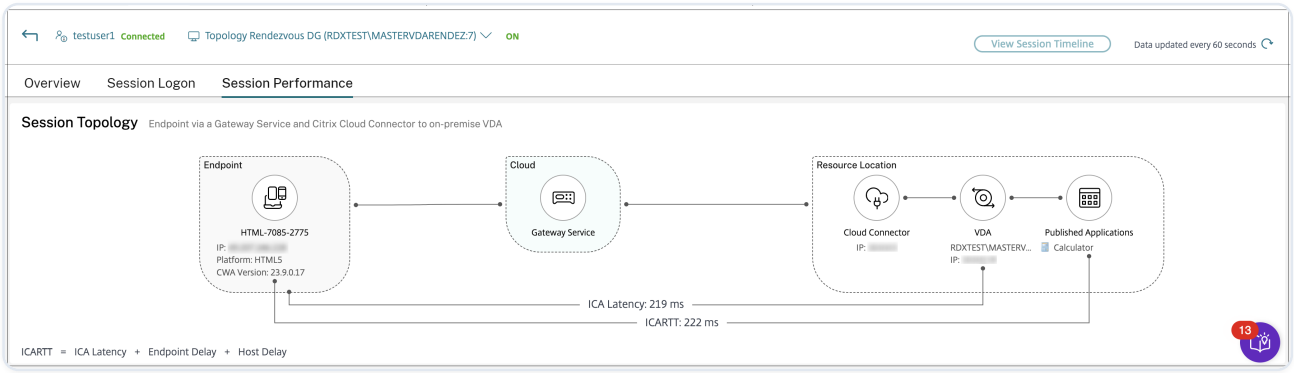
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Accordingly, the possible network topologies are as follows:

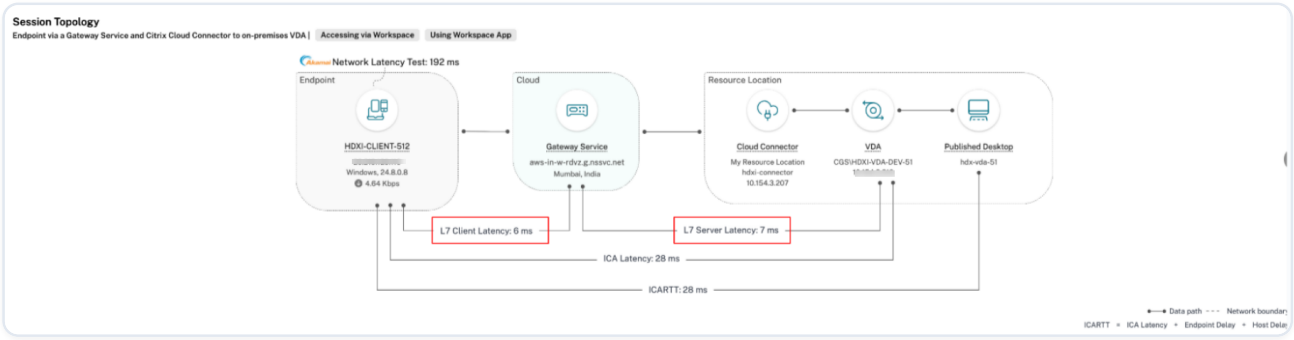
- Citrix Workspace app on the endpoint connects via Citrix® StoreFront Cloud and Gateway Service to an on-premises VDA. No Cloud Connector is used to connect to VDA.



- Citrix Workspace app on the endpoint connects via Citrix® StoreFront Cloud and Gateway Service to an on-premises VDA via Cloud Connector.

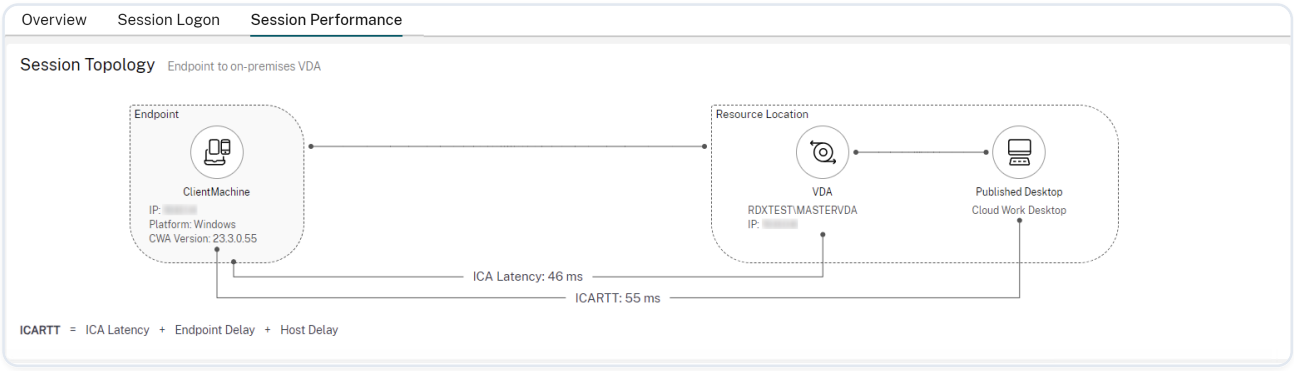


- Citrix Workspace app on the endpoint connects via StoreFront™ and on-premises Gateway to on-premises VDA.



- Citrix Workspace app on the endpoint connects via StoreFront to on-premises VDA.

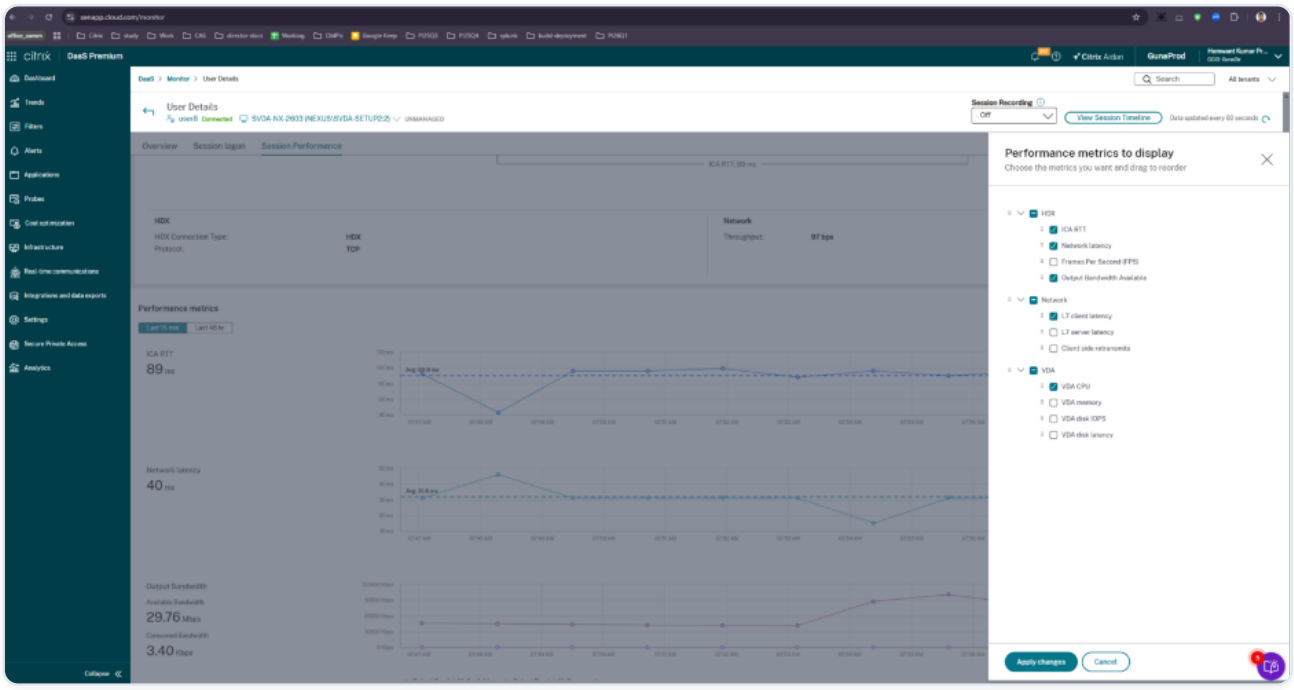
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Performance Metrics

The **Performance Metrics** panel offers the ability to correlate real-time metrics in identifying issues within user sessions. Trends for the session metrics help indicate how these metrics have performed over time. When you click the **Session Performance** tab, along with the real-time data, you can view the last 15 minutes and 48 hours data. The plots help to correlate multiple component performance metrics in a single view.

Use the *Manage* option in this section to choose the relevant metrics you want to visualize and correlate for the given user.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- With the trailing 15-minutes metrics support, the graph is plotted for the duration for which the session is connected and disconnected. The disconnected session's metric is displayed with the value zero.
- With the trailing last 48 hours metrics support, the ICARTT, ICA Latency, and Session Reconnects plots are updated with the historical data metrics. The session reconnect information helps you to view and troubleshoot network connections having interruptions. It also analyzes networks having a seamless experience. The graph to see the number of Session Reconnects, Total Session Reconnects, Auto client reconnect, and Session reliability reconnects.

Apart from ICARTT and ICA Latency, the following metrics are available for real-time and last 15-minutes metrics:

- Frames Per Second - Frames Per Second is an important metric that indicates the session responsiveness.
- Output Bandwidth Available - Output Bandwidth Available is a measure of the total bandwidth available to transmit data from the VDA to the endpoint.
- Output Bandwidth Consumed - Output Bandwidth Consumed indicates the actual amount of data transmitted from the VDA to the endpoint to display sessions to users.

Analyzing Output Bandwidth Available and the Output Bandwidth Consumed helps check if sufficient bandwidth is available to serve sessions and to detect if a session is affected by insufficient bandwidth.

Troubleshoot when ICA RTT or Session Logon Duration data fails to populate

Previously, when EUEM service or Profile Management service failed to run, the reason for failure in getting the data related to ICA RTT or Session Logon Duration wasn't displayed. With this new feature, you can get the reason for failure and the corresponding solution for that failure. The **Learn more** links provides the ICA RTT and Session Logon Duration errors, the reason for failure, and the solution as mentioned in the following table:

ERROR TYPE	ERROR	ERROR MESSAGE	SOLUTION
ICA RTT error	ICA RTT value is not displayed.	**Citrix End User Experience**	`1.` Open the Services console. To

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR TYPE	ERROR	ERROR MESSAGE	SOLUTION
		Monitoring is not running.	open this console, click **Start** and then type **Services**.
			`2.` Make sure that the Citrix End User Experience Monitoring Service is running.
			`3.` Reopen the desktop session and try. The ICA RTT value must be displayed.
			`4.` If the issue persists, contact the Citrix administrator.
ICA RTT error	ICA RTT value is not displayed.	**Citrix End User Experience Monitoring is not installed.**	`1.` Re-install the VDA.
			`2.` Open the Services console. To open this console, click **Start** and then type Services
			`3.` Make sure that the Citrix End User Experience Monitoring Service is running.
			`4.` Reopen the desktop session and try. The ICA RTT value must be displayed now.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR TYPE	ERROR	ERROR MESSAGE	SOLUTION
			`5.` If the issue persists, contact the Citrix administrator.
ICA RTT error	ICA RTT value is not displayed.	**Error fetching data.**	`1.` Open the Services console. To open this console, click **Start** and then type Services.
			`2.` Ensure that the **Windows Management Instrumentation Service** is running.
			`3.` Also, ensure that the WfShell.exe/ PicaShell.exe process is running under **Activity Manager** > **Process** tab. If it is not running, reopen the desktop session.
			`4.` If the preceding steps are not working, run the following command to ensure that the Citrix_Euem_Round Trip instance is present: `Get-CimInstance -Namespace 'ROOT\Citrix\Euem' -Query "select * from`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR TYPE	ERROR	ERROR MESSAGE	SOLUTION
			`Citrix_Euem_RoundTrip"`
			`5.` If the Citrix_Euem_RoundTrip instance is present, reopen the desktop session.
			`6.` If the issue persists, contact the Citrix administrator.
Session Logon Duration error	The graph is not loaded.	**Citrix Profile Management is not running**	`1.` Open the Services console. To open this console, click **Start** and then type Services.
			`2.` Ensure that the **Citrix Profile Management Service** is running.
			`3.` Reopen the desktop session and try. The graph must be displayed.
			`4.` If the issue persists, contact the Citrix administrator.
Session Logon Duration error	The graph is not loaded.	**Citrix Profile Management is not installed.**	`1.` Install the Citrix Profile Management Service.
			`2.` Open the Services console. To open this console,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR TYPE	ERROR	ERROR MESSAGE	SOLUTION
			click **Start** and then type Services. `3.` Ensure that the **Citrix Profile Management Service** is running. `4.` Reopen the desktop session and try. The graph must be displayed. `5.` If the issue persists, contact the Citrix administrator.
Session Logon Duration error	The graph is not loaded.	**Error fetching data.**	`1.` Open the **Services** console. To open this console, click **Start** and then type Services. `2.` Ensure that the **Windows Management Instrumentation Service** is running. `3.` If the preceding service is already running, run the following command to ensure that the `LogonTimings instance is present`: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics'`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR TYPE	ERROR	ERROR MESSAGE	SOLUTION
			`-Query "select * from LogonTimings"`
			`4.` If the issue persists, contact the Citrix administrator.
ICA RTT error	ICA RTT value is not displayed.	Console isn't supported.	Start a session using HDX.
ICA RTT error	ICA RTT value is not displayed.	Remote Desktop Protocol (RDP) isn't supported.	Start a session using HDX.
ICA RTT error	ICA RTT value is not displayed.	Upgrade VDA to version 2402 or higher to get detailed error detection and access all the features.	Upgrade VDA to 2402 or higher.
Session Logon Duration error	The graph is not loaded.	Citrix Profile Management WMI plug-in isn’t installed.	Install Citrix Profile Management WMI plug-in.

Diagnose application performance issues

Application Performance monitoring in Citrix Director (integrated with uberAgent) provides administrators with granular insights into how individual applications—both published and local—are performing. This data helps you identify whether an issue is caused by the application's resource consumption, network dependencies, or UI unresponsiveness.

Prerequistes

- VDA Windows version should be greater than or equal to 2603
- uberAgent must be installed on the VDAs
- The policy "Enhance Director with uberAgent data for application performance "must be enabled on the studio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLICY NAME	POLICY DESCRIPTION	UI METRICS	DEFAULT VALUE	VALUE OPTIONS	VDA WINDOWS VERSION	VDA (LINUX, MAC)
Enhance Director with uberAgent data for application performance	Enable Director to use machine metrics data provided by uberAgent for application performance	Application name, Is published, Process name, CPU usage %, Memory usage %, Working set memory (MB), Disk IOPS, Disk latency (ms), Network latency (ms), Input delay (ms), CPU usage % (P95), Memory usage % (P95), Input delay (P95) (ms), Page fault	Enabled	Enabled or Disabled	2603 or later	Not Available

© 1997–2026 Citrix Systems, Inc. All rights reserved.

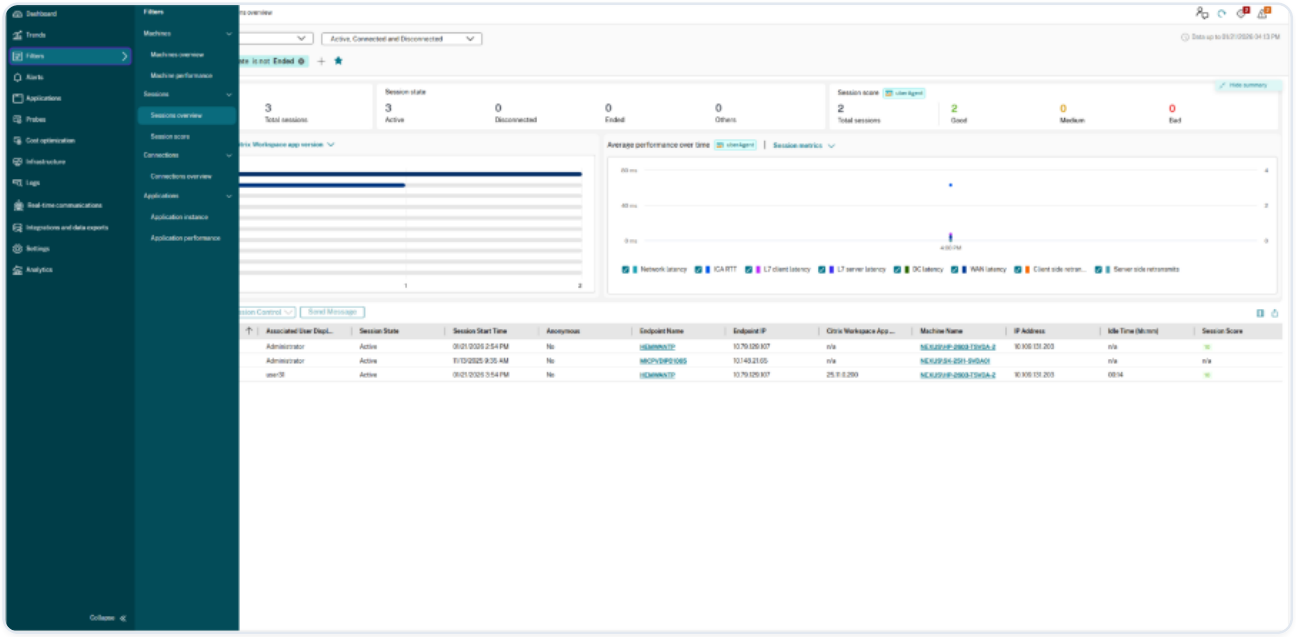
POLICY NAME	POLICY DESCRIPTION	UI METRICS	DEFAULT VALUE	VALUE OPTIONS	VDA WINDOWS VERSION	VDA (LINUX, MAC)
		per second				

Overview and Key Features

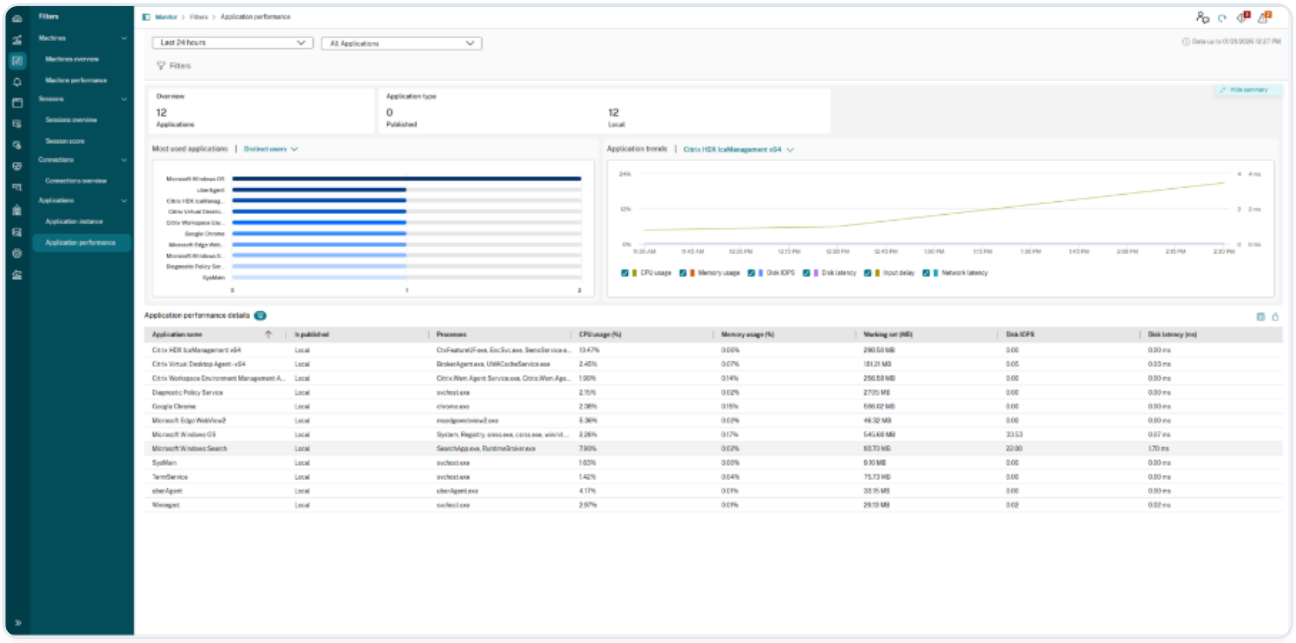
This page details the documentation for the new **Application Performance** tab, which focuses on real-time and historical monitoring of both published and local applications.

The key features are:

- Time Range Filters: Enhanced monitoring precision with time range options.
- Streamlined Filter Management: Intuitive dropdown for managing filters.
- Intuitive Filter Building: Flexible workflow for creating and modifying filters directly on the main page.
- Visualizations: Introduction of the Application Distribution chart and Performance Over Time chart for immediate insight into application performance trends.



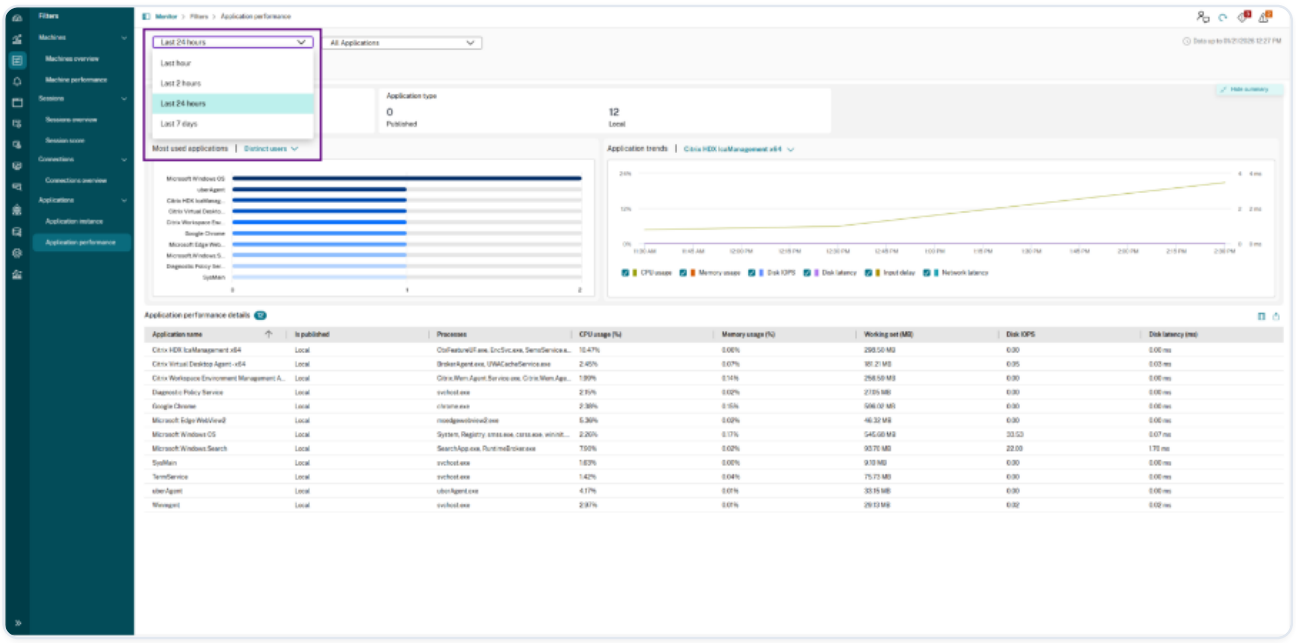
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Filtering Data

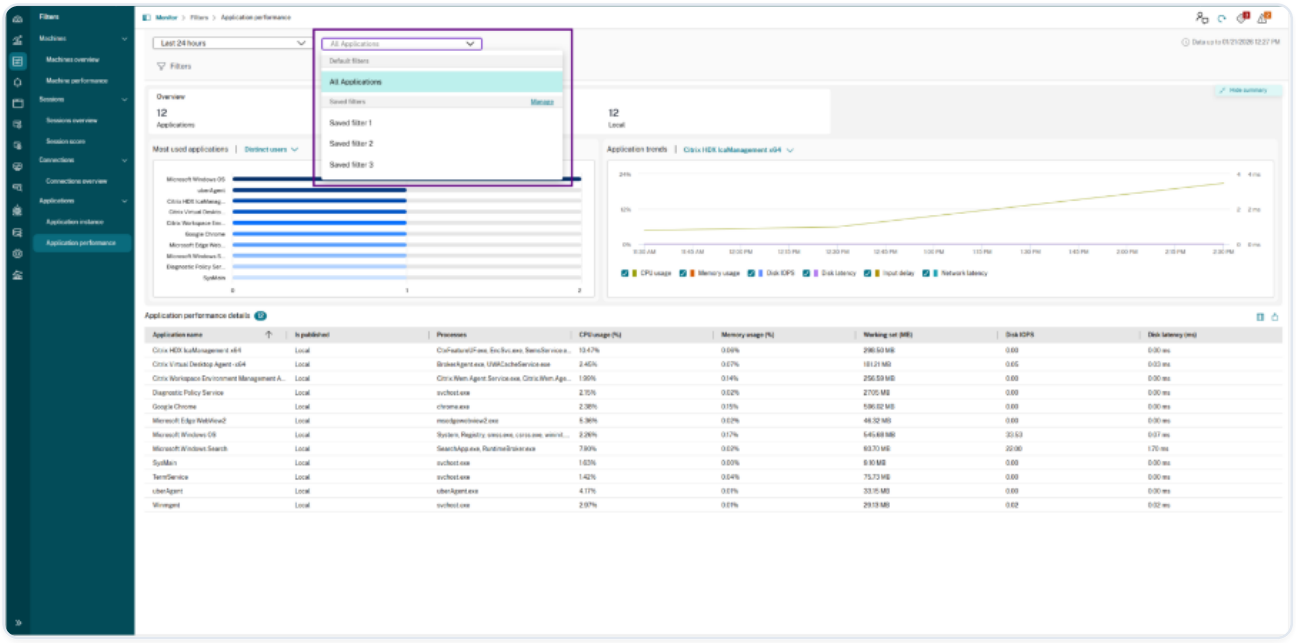
At the top of the page, you can define the scope of the data displayed.

- **Time Period:** Choose the time range. The time range filter includes 1 hour, 2 hours, 1 day or seven days

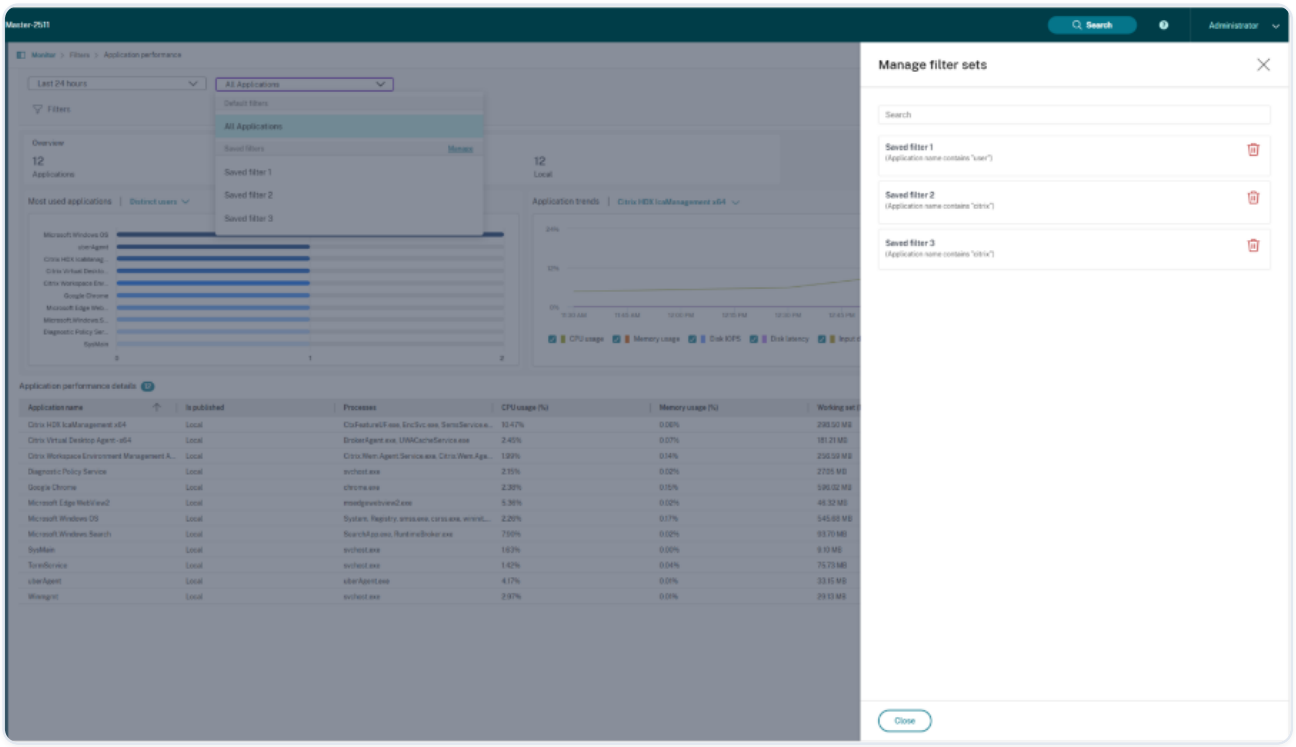


- **Application Scope:** Use the application dropdown to filter the entire dashboard by a specific filter or view **All Applications**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Filters:** Use the Filters icon to further refine data.
- **Manage:** Clicking Manage opens a side panel where you can search for, view, or delete existing saved filters.

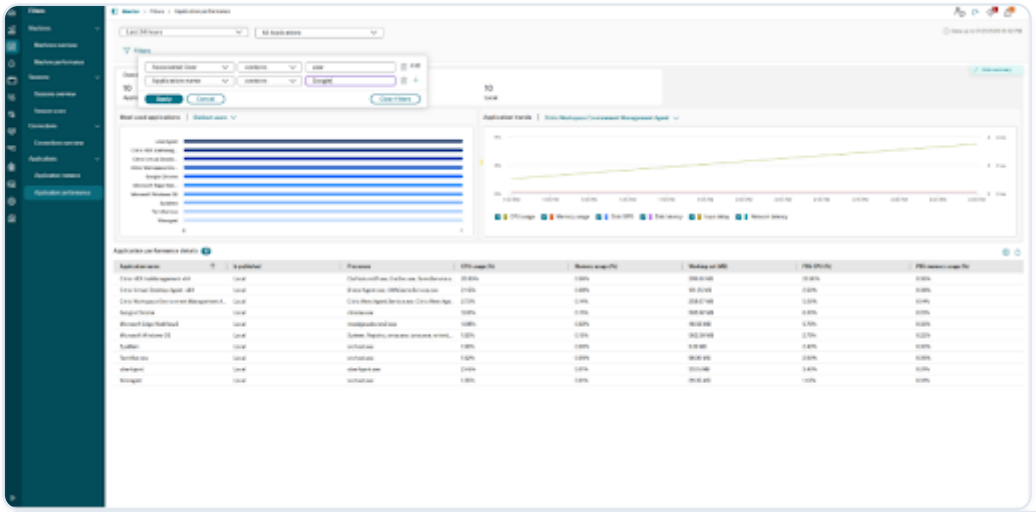


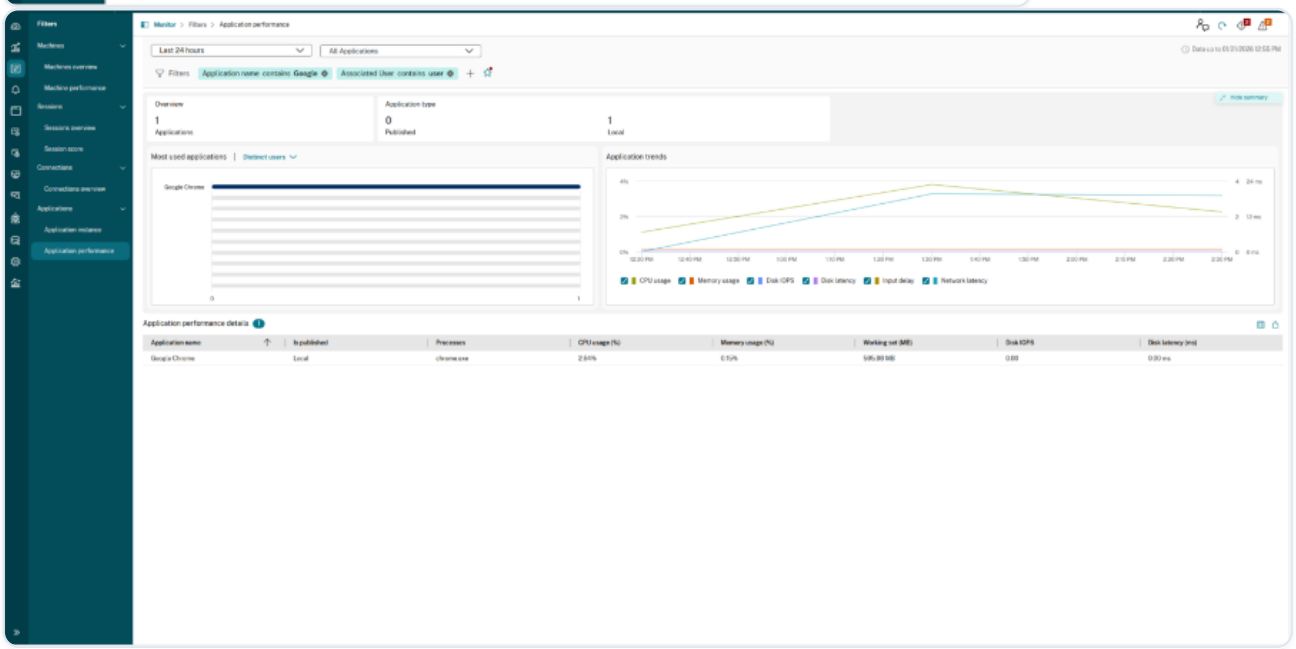
Building and Applying Filters

You can now build complex filter sets directly on the applications overview page:

- Click the Filters icon or the + button next to an existing filter.
- Select the criteria (e.g., Application name), the operator (e.g., contains), and the value (e.g., Google).

© 1997–2026 Citrix Systems, Inc. All rights reserved.





FILTER SAVE STATUS AND WORKFLOW

The star icon (⋆) next to the active filters visually indicates the status of your current filter set. This helps to guide admins for saving, applying, and managing custom filters.

FILTER STATUS	ICON APPEARANCE	MEANING	REQUIRED ACTION
Unsaved Filter	☐ (Empty outline with a Red Dot)	The current combination of filter criteria has **not been saved**.	Click the **empty star** to open the dialog box, name the filter set, and save it.
Saved Filter	☐ (Filled / Solid)	The currently active filter set is an **exact match** to a previously saved filter.	No action required. You are viewing data based on a defined template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FILTER STATUS	ICON APPEARANCE	MEANING	REQUIRED ACTION
Saved Filter with Changes	 (Filled with Red Dot)	When using a **saved filter**, any other filter is added, removed, or if any column is sorted then the red dot appears which means the changes are **not yet saved**.	Click the **red-dotted star** to update the existing saved filter, or use the dropdown to select **Save as filter set** to create a new one.

FILTER ACTION BUTTONS

When adding new filters or modifying a saved filter, the following controls and status indicators become available:

BUTTON	MEANING AND ACTION
Update	Applies all currently active filter criteria to the charts and the application performance data table.
Cancel	Discards any changes made to the current filter set and reverts to the last applied filter.
Clear filters	Removes all the newly added filter criteria.
 **Icon**	Removes the selected filter criteria on which this icon is clicked.

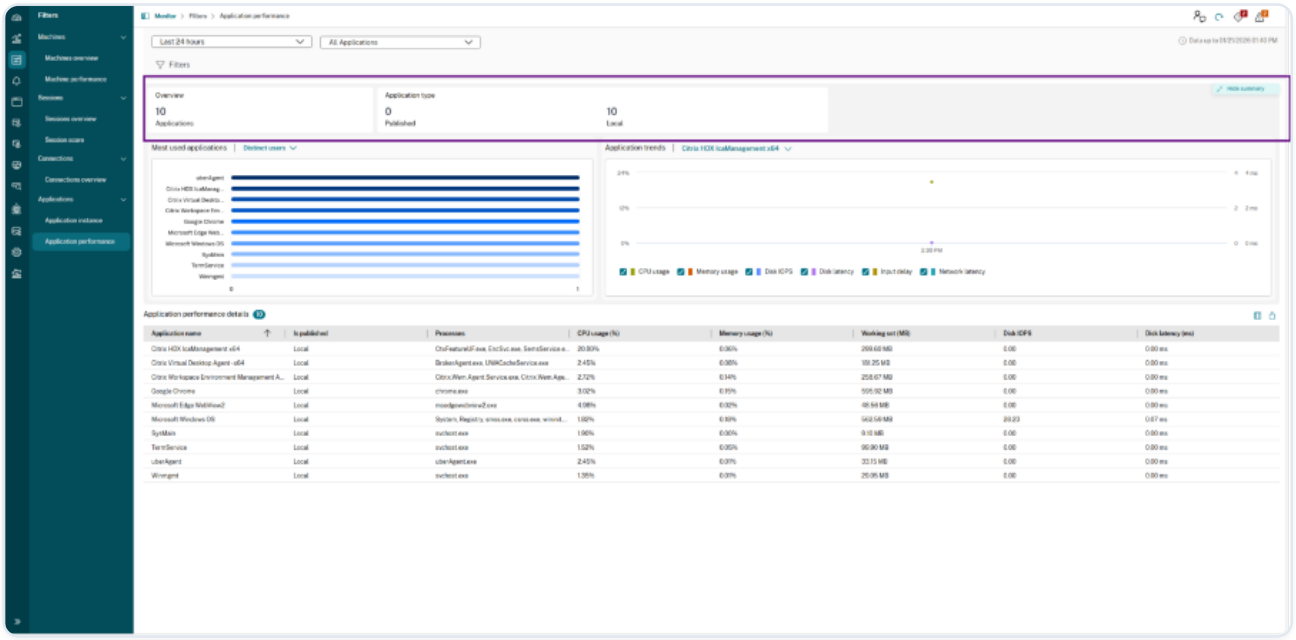
Visualization

OVERVIEW SUMMARY

The summary pane provides an immediate count of the applications currently being monitored:

- **Applications:** The total number of unique application names detected in the environment.
- **Application Type:** A breakdown of how many is **Published** applications versus **Local** applications running on the VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

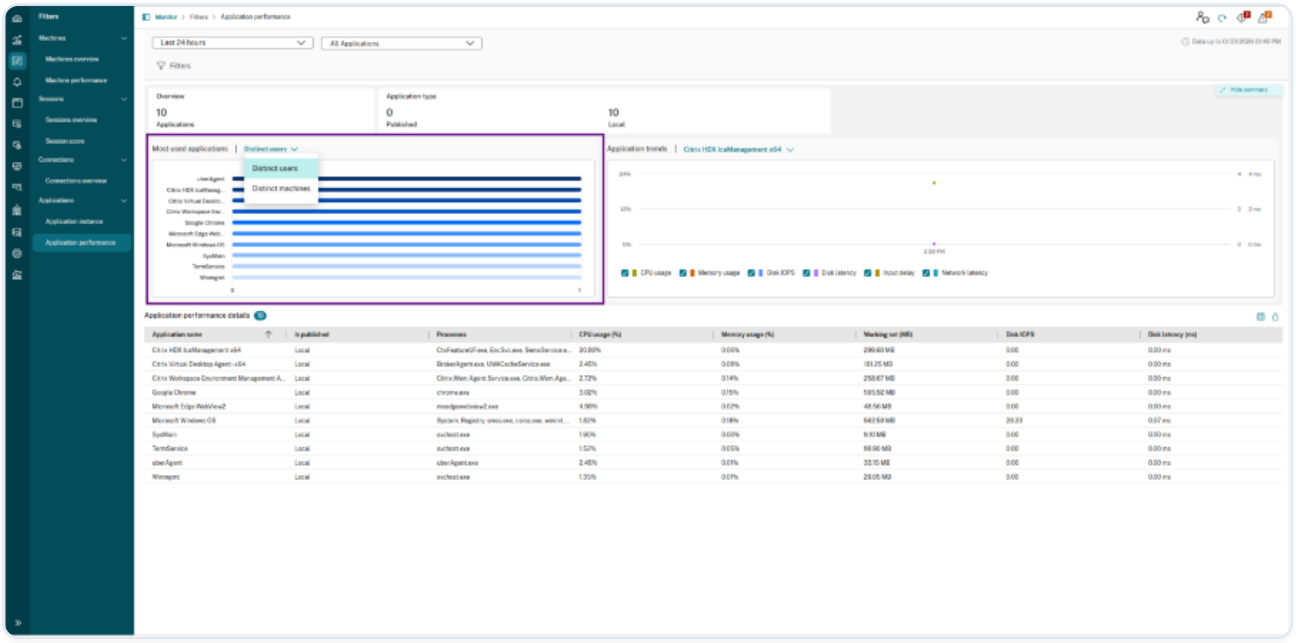


Distribution Chart

The Distribution chart serves as a histogram that categorizes the number of application instances based on specific performance buckets. It is designed to help you understand the "spread" of the user experience across your environment.

- **Metric Grouping:** The X-axis represents ranges of the selected metric (such as **UI Delay** or **Startup Duration**), while the Y-axis represents the count of occurrences within those ranges.
- **View Perspectives:** A drop-down menu allows you to toggle the data representation between two views:
  - **Distinct Users:** Shows the distribution of performance based on the number of unique users
  - **Distinct Machines:** Shows the distribution based on the number of VDAs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

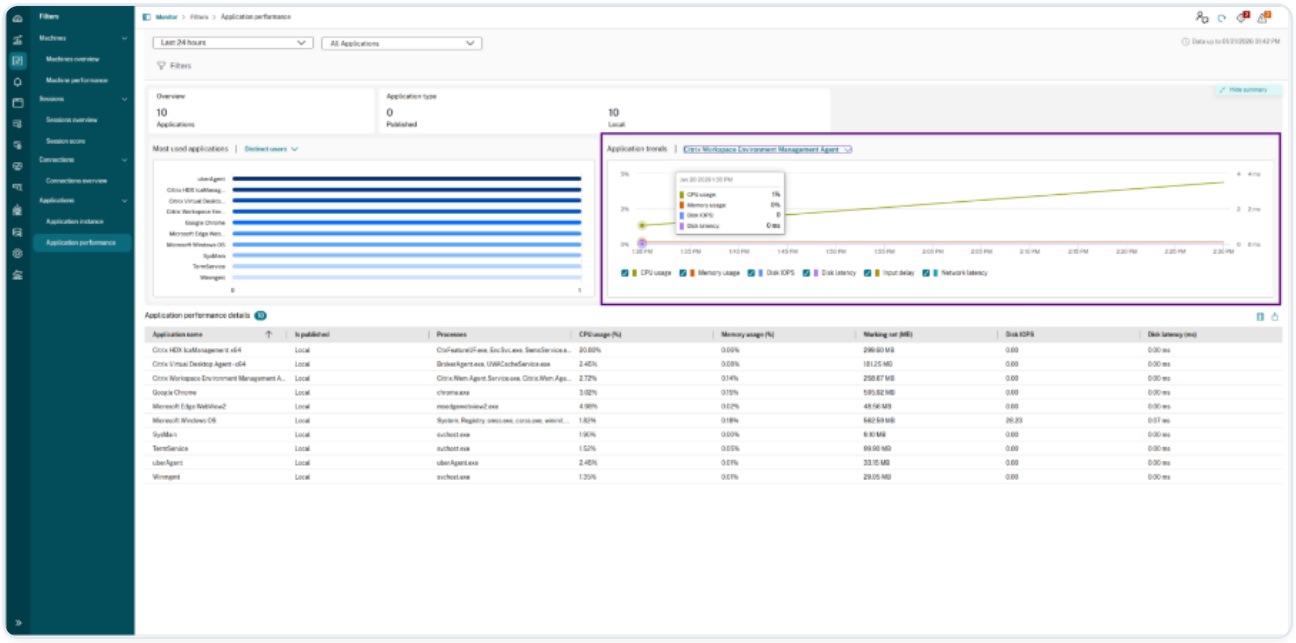


Performance Chart

The Performance chart is a time-series visualization that tracks application health over a selected duration. It allows you to correlate performance changes with specific time intervals and resource consumption.

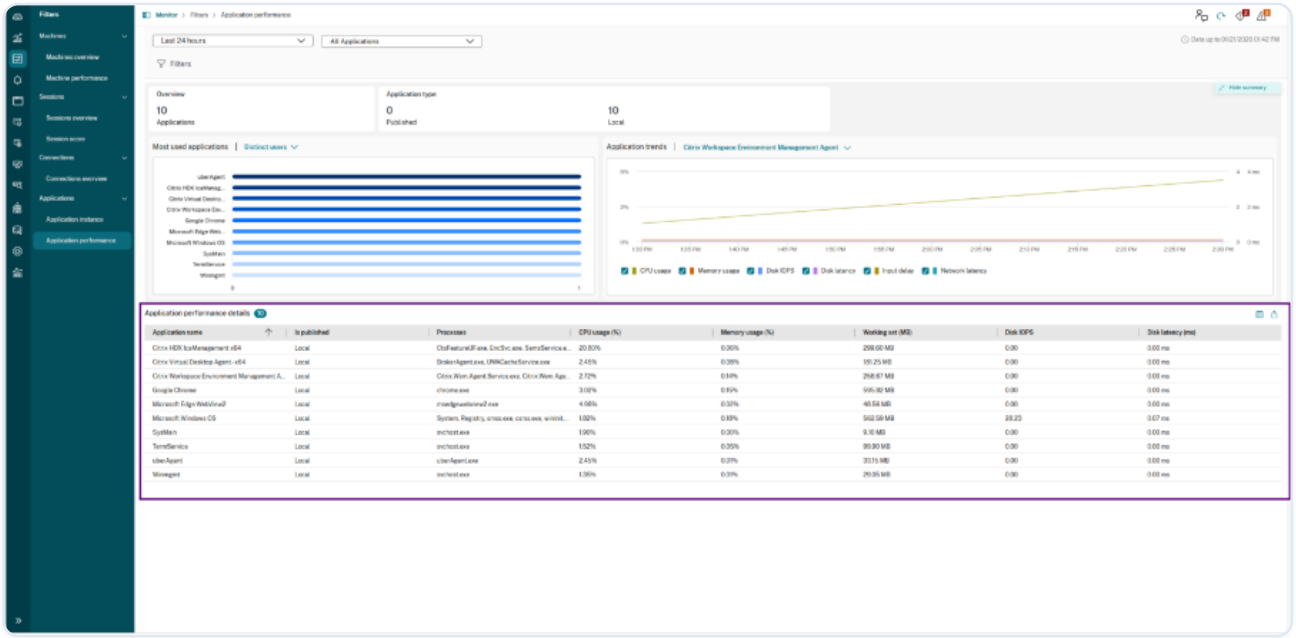
- **Application Selection:** Use the drop-down menu at the top of the chart to select a specific application to analyse.
- **Multi-Metric Correlation**: The chart allows you to overlay several key performance indicators (KPIs) simultaneously to find correlations between responsiveness and resource usage:
  - **CPU and Memory Usage**: Displays the percentage of resource consumption by the application.
  - **Disk IOPS and Disk Latency**: Identifies if storage bottlenecks are impacting application performance.
  - **Input Delay**: Measures the time between a user action and the application's response.
  - **Network Latency**: Tracks the network delay associated with the application's communication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

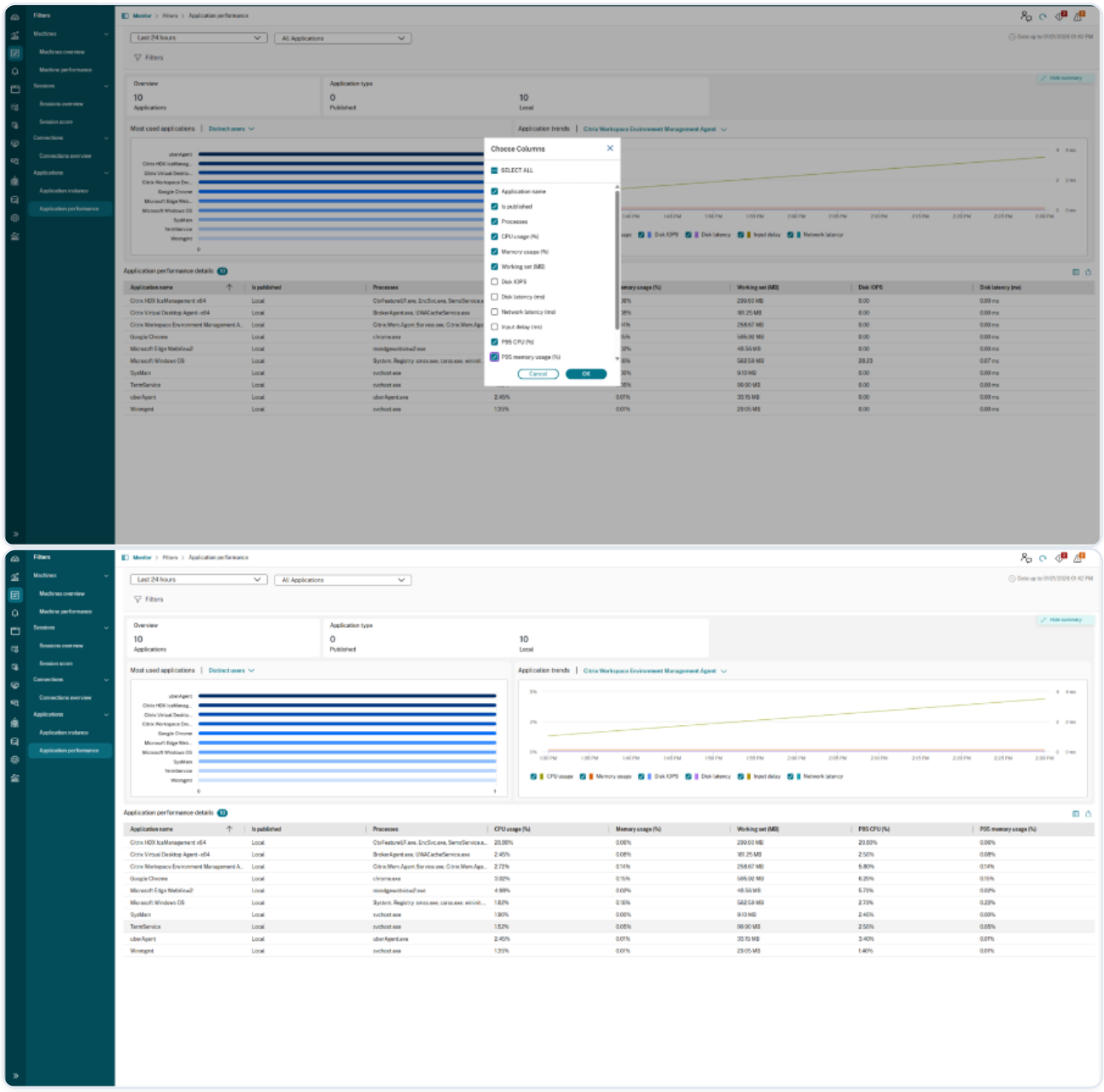


Application Performance Details (Table)

The bottom pane provides the raw, actionable data for every application instance. The data can be exported, and the desired columns can be chosen to be displayed.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Diagnose historical user sessions

Citrix Monitor now displays the details of sessions in active, disconnected, or in terminated state. Previously, you could see the details of active sessions only. With this feature, help desk admins can troubleshoot issues with a session that was ended or in a terminated state. The details for ended sessions are available for the last 24 hours and last 2 days. You can view the following details of an ended or terminated session:

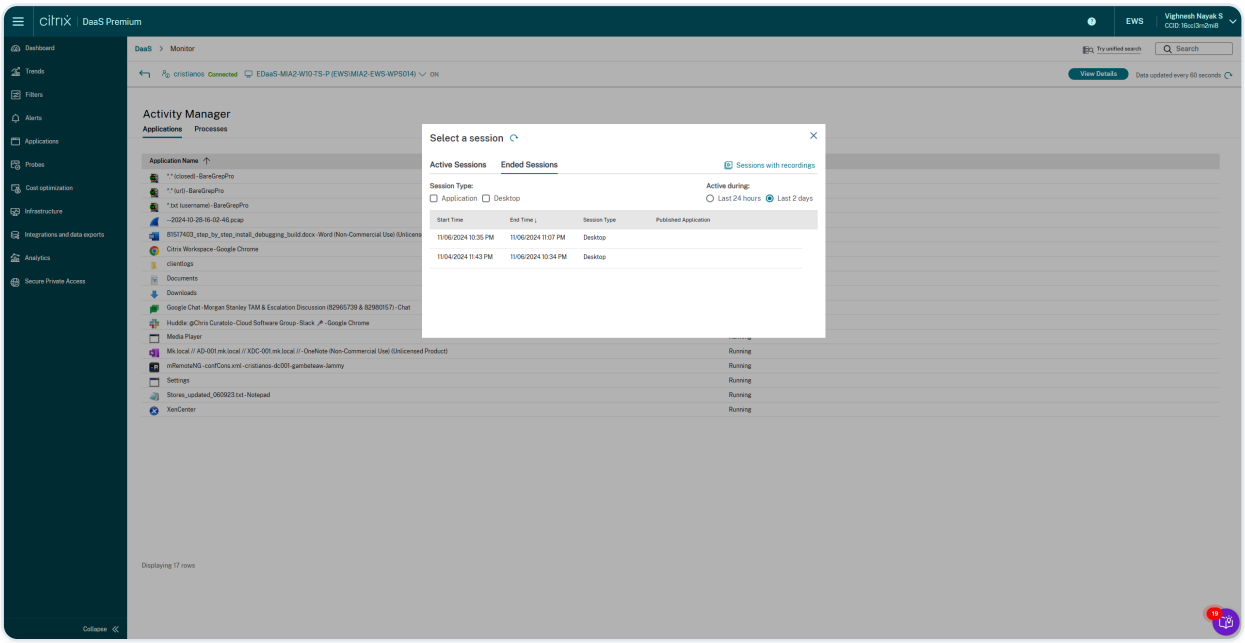
- Machine Details panel - Displays the available details of the machine where the selected session was launched
- Session Details panel - Displays the available details of the selected session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Session logon duration - Displays the information on the logon duration taken for the selected session. You can view the chart on time taken for the following:
  - Brokering
  - Machine start-up
  - HDX™ connection
  - Authentication
  - GPOs
  - Logon scripts
  - Profile load on disk
  - Interactive session

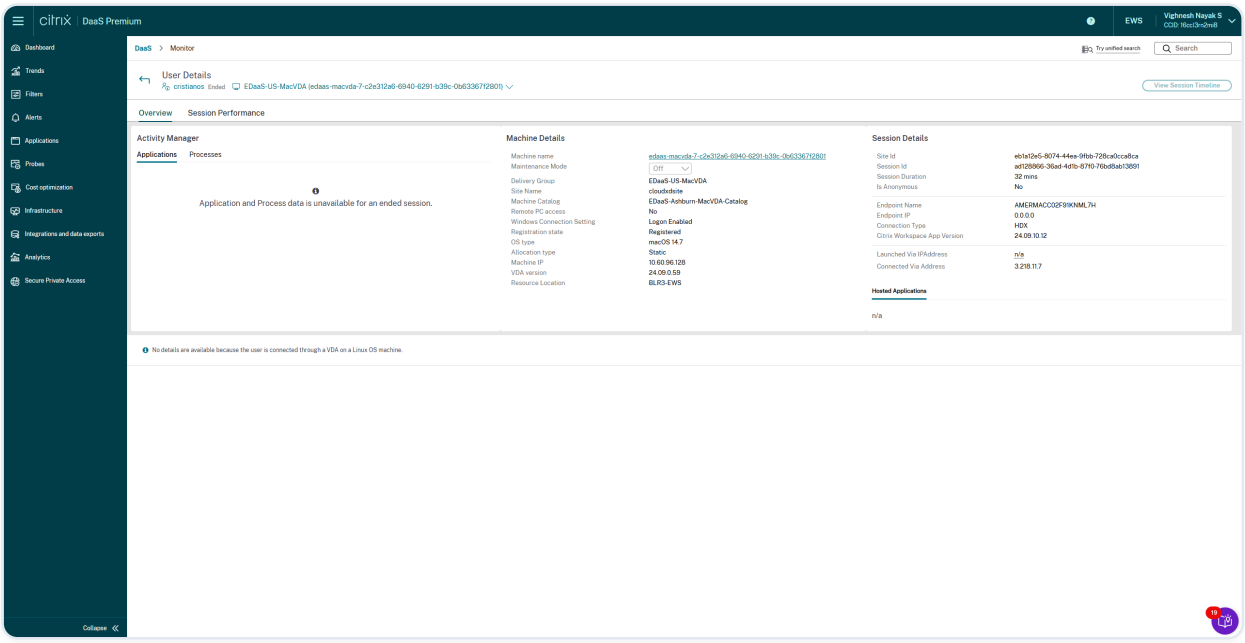
To view the historical user sessions, do the following:

1. Click **Filter** > **Session** view.
2. Click the **Associated User** to open the Activity Manager for the user.

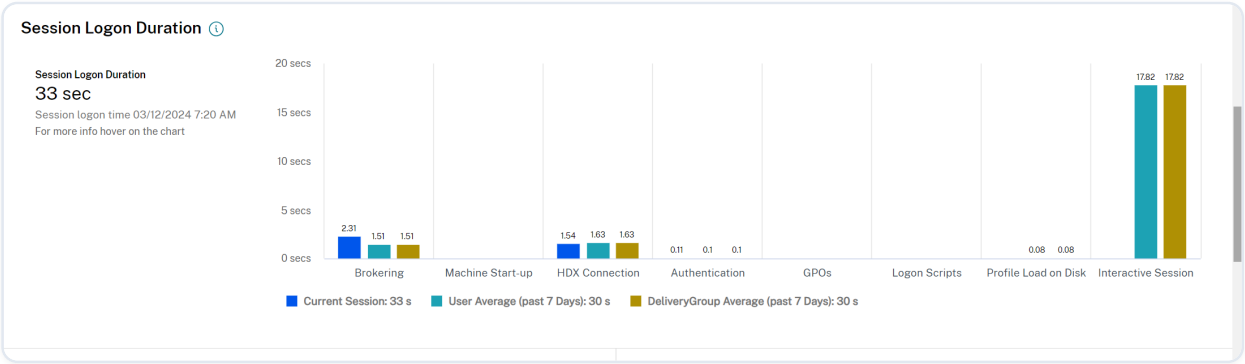


3. Select the required session from the **Ended Sessions** section.
4. View the **Machine Details** and **Session Details** panels.

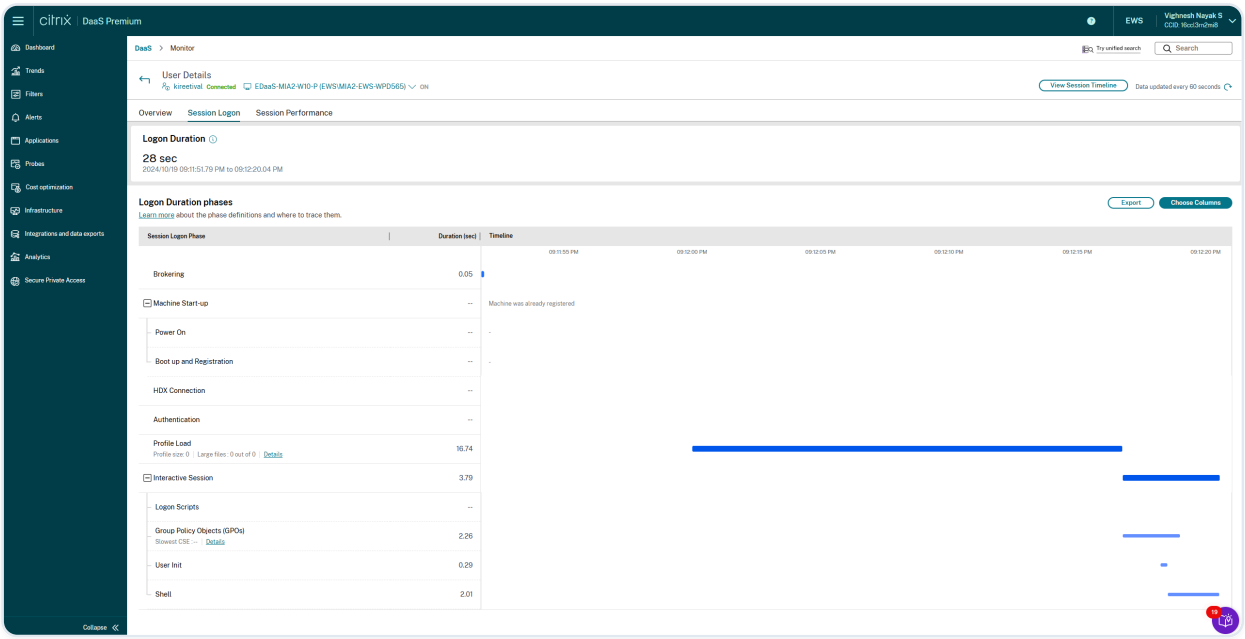
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Scroll down and view the **Session logon duration** for the ended session.

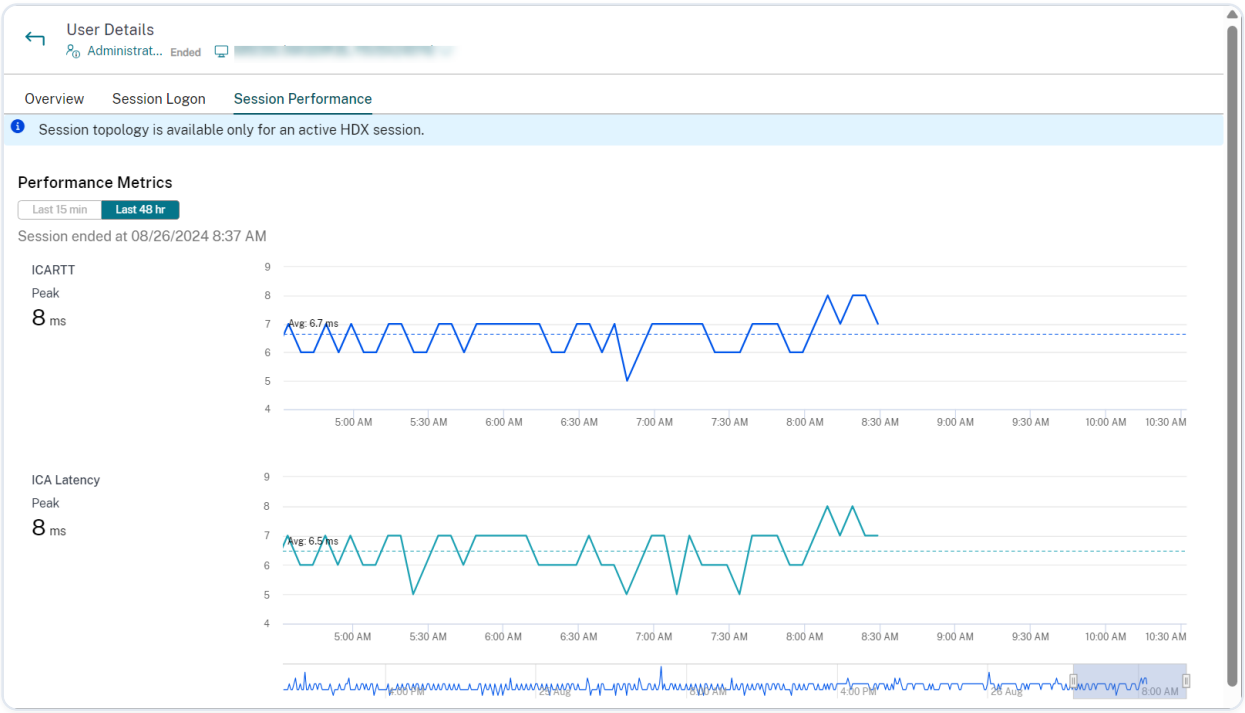


6. Click the **Session Logon** tab and view the details.



7. Click the **Session Performance** tab and view the details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Shadow users

Use the shadow user feature to view or work directly on a user's virtual machine or session. You can shadow both Windows or and Linux VDAs. The user must be connected to the machine that you want to shadow. Verify this by checking the machine name listed in the user title bar.

Shadowing is launched in a new tab, update your browser settings to allow pop-ups from the Citrix Cloud™ URL.

Access the shadowing feature from the **User Details** view. Select the user session, and click **Shadow** in the Activity Manager view or the Session Details panel.

Shadowing Linux VDAs

Shadowing is available for Linux VDAs Version 7.16 or and later running the RHEL7.3 or Ubuntu Version 16.04 Linux distributions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Monitor uses FQDN to connect to the target Linux VDA. Ensure that the Monitor client can resolve the FQDN of the Linux VDA.
- The VDA must have the python-websockify and x11vnc packages installed.
- noVNC connection to the VDA uses the WebSocket protocol. By default, **ws://** WebSocket protocol is used. For security reasons, Citrix recommends that you use the secure **wss://** protocol. Install SSL certificates on each Monitor client and Linux VDA.

Follow the instructions in Session Shadowing to configure your VDA for shadowing.

1. After you click **Shadow**, the shadowing connection initializes and a confirmation prompt appears on the user device.
2. Instruct the user to click **Yes** to start the machine or session sharing.
3. The administrator can only view the shadowed session.

Shadowing Windows VDAs

Windows VDA sessions are shadowed using Windows Remote Assistance. Enable User Windows Remote Assistance feature while installing the VDA. For more information, see Enable or Disable features.

1. After you click **Shadow**, the shadowing connection initializes and a dialog box prompts you to open or save the .msrc incident file.
2. Open the incident file with the Remote Assistance Viewer, if not already selected by default. A confirmation prompt appears on the user device.
3. Instruct the user to click **Yes** to start the machine or session sharing.
4. For more control, ask the user to share keyboard and mouse control.

STREAMLINE MICROSOFT INTERNET EXPLORER BROWSERS FOR SHADOWING

Configure your Microsoft Internet Explorer browser to automatically open the downloaded Microsoft Remote Assistance (.msra) file with the Remote Assistance client.

To do this, you must enable the Automatic prompting for file downloads setting in the Group Policy editor:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Computer Configuration \> Administrative Templates \> Windows Components \> Internet Explorer \> Internet Control Panel \> Security Page \> Internet Zone \> Automatic prompting for file downloads.

Using HDX Screen Share

Director supports remote assistance that enables IT administrators and helpdesk personnel to provide remote support to end users through HDX screen sharing technology. This feature leverages Citrix's native HDX protocol to deliver secure, high-performance screen sharing capabilities for troubleshooting and user assistance scenarios.

PREREQUISITES

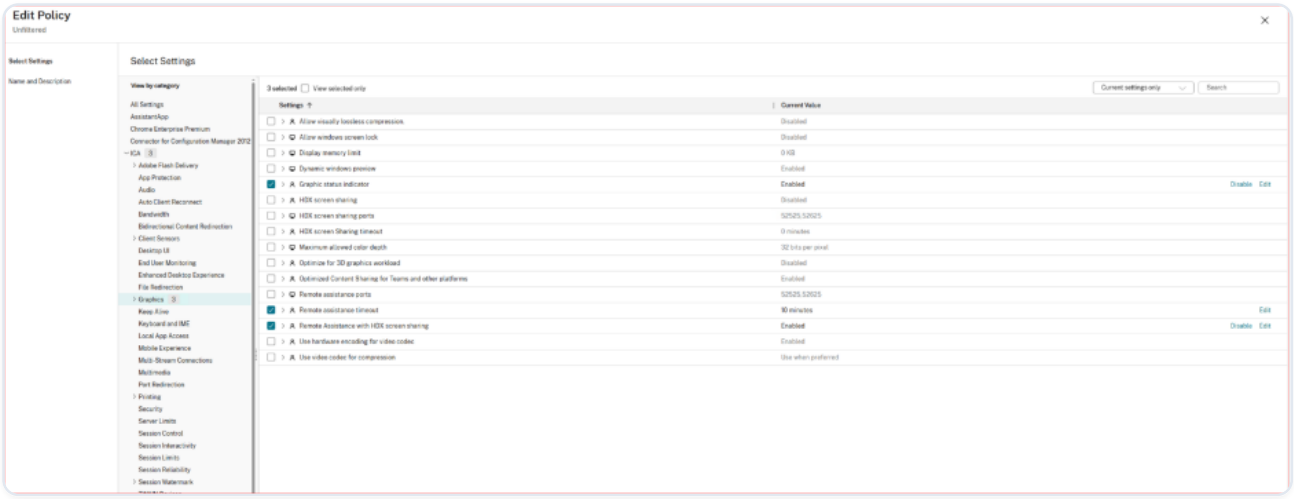
COMPONENT	SUPPORTED ENVIRONMENTS OR VERSIONS
Operating Systems	Windows, Linux for Single Session OS **or Multi Session OS**
Virtual Delivery Agent (VDA)	CR 2511 or above
Director	CR 2511 or above
Delivery Controller	CR 2511 or above
TWPlayer (ThinWire Player)	A link to download the player is available on the Director UI when initiating a shadow session

GROUP POLICY CONFIGURATION

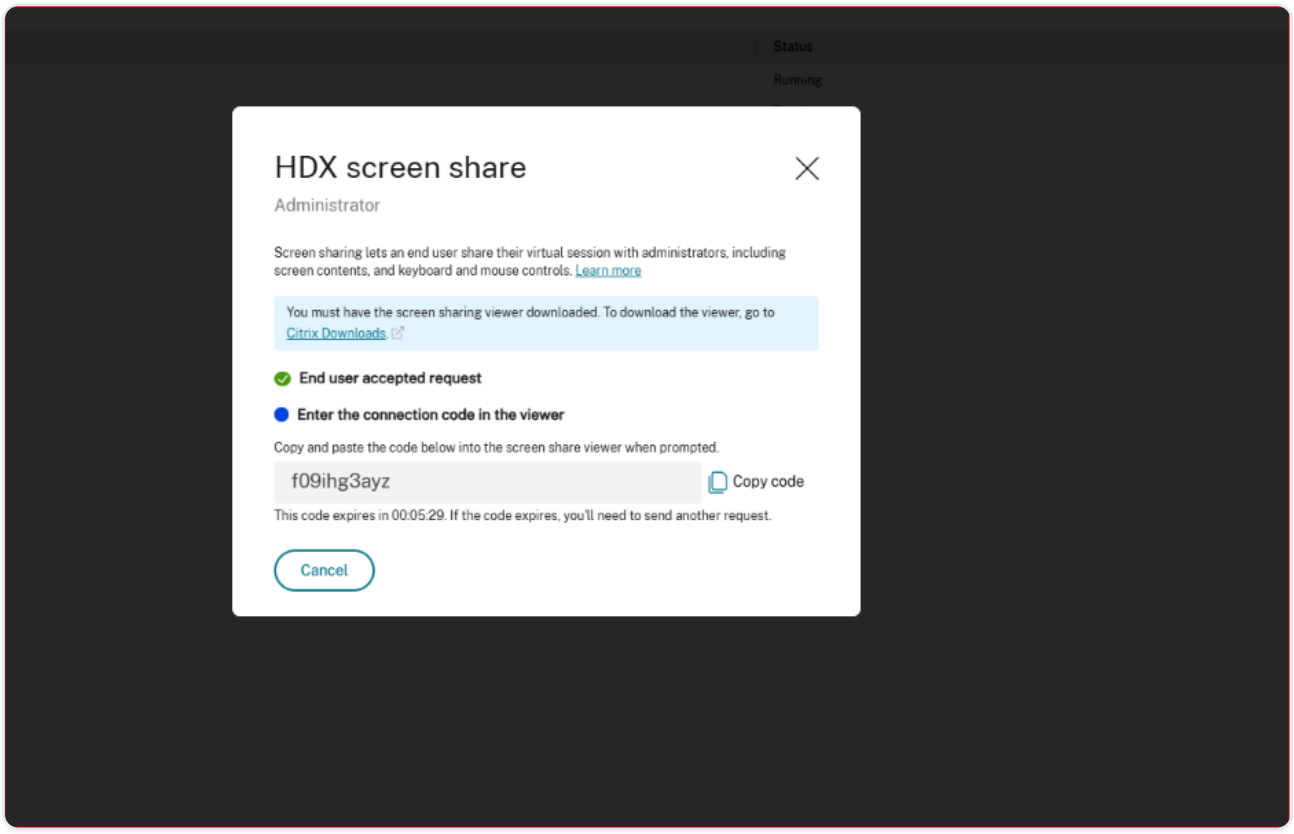
To enable Remote Assistance using Director and HDX Screen Share, configure the following Group Policies on the VDA:

- Remote Assistance with HDX screen sharing
- Remote assistance timeout
- Graphics Status Indicator

© 1997–2026 Citrix Systems, Inc. All rights reserved.



TWPlayer (ThinWire Player) is a required component that must be downloaded once to enable HDX screen sharing functionality. A link to download the player is available on the Director UI when initiating a shadow session.



Limitations

- Published applications (app sessions) cannot be shadowed – desktop sessions only.

Workflow using Director and HDX Screen Share

The steps below outline the process for an administrator to initiate an HDX screen share session:

1. **Initiate Shadow Session**

    a. Log in to Citrix Director

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Navigate to user session requiring assistance

c. Click the "Shadow " button

d. Choose HDX Screen share

2. **Launch Viewer**

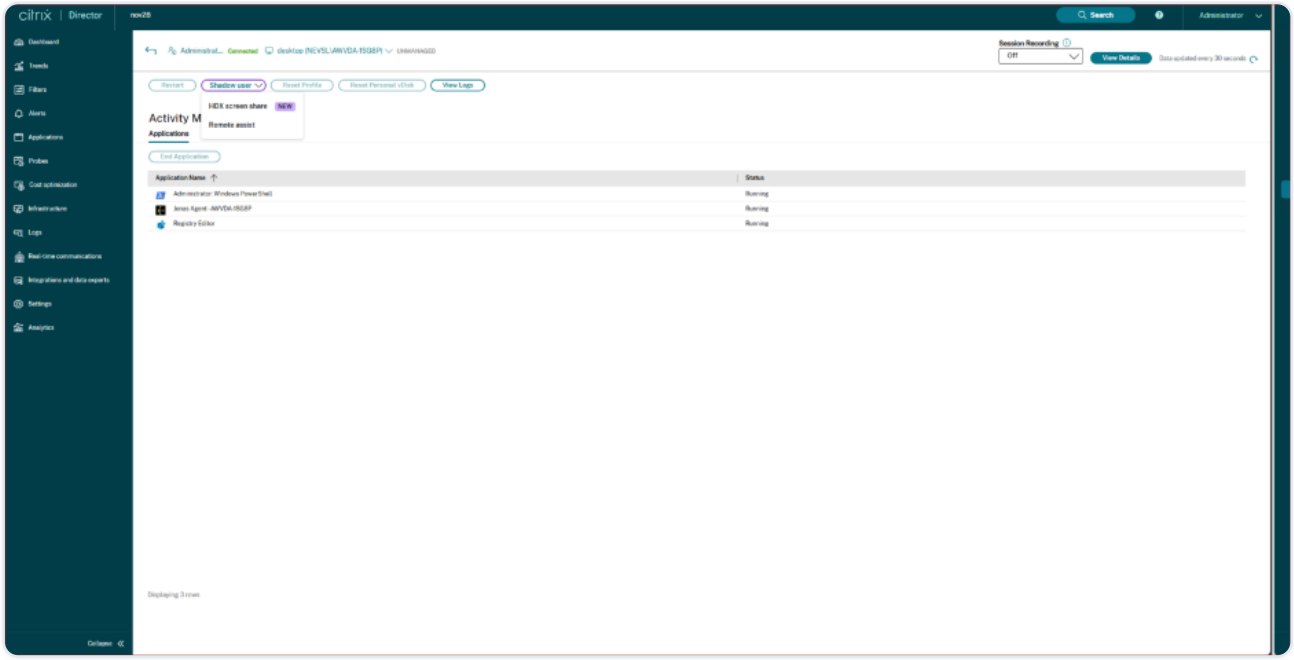
a. Open the generated incident file with TWPlayer/Remote Assistance Viewer

b. Wait for user to accept the connection request

3. **View Session**

a. Session screen appears in the viewer window

b. Administrator can observe user actions in real-time



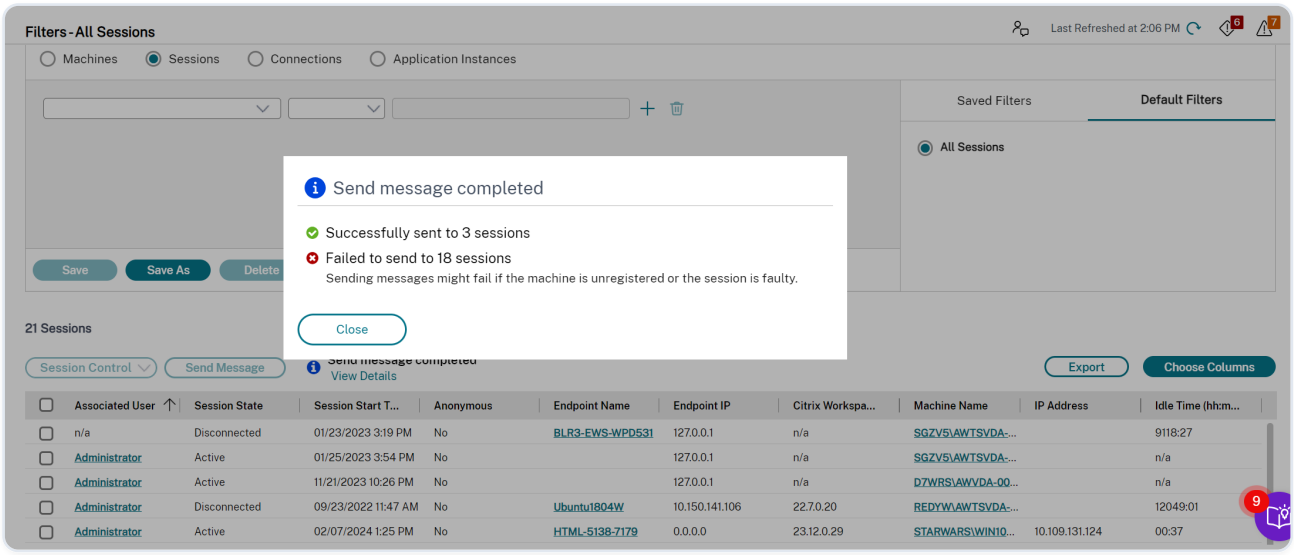
Send messages to users

From Monitor, send a message to a user who is connected to one or more machines. For example, use this feature to send immediate notices about administrative actions such as impending desktop maintenance, machine logoffs and restarts, and profile resets.

To send a message to a user, follow these steps:

1. Go to **Monitor** > **Filters** > **Machines** > **All Machines**.
2. Select a machine to which you want to send a message and click **Send Message**.
3. Type your message and click **Send**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Sending messages can fail if the machines are unregistered or if the sessions are faulty.

If the message is sent successfully, a confirmation message appears. If the user's machine is connected, the message appears there.

If the message is not sent successfully, an error message appears. Troubleshoot the problem according to the error message. When you have finished, type the subject and message text again and click **Try again**.

If you choose to send bulk messages to all connected sessions, the progress of the operation is displayed in percentage. Once the operation is completed, the number of messages that were successfully sent and the number that have failed are displayed. Send message status is specifically helpful when you are administering large sites. It helps understand if the message needs to be resent to certain users.

Custom role to limit bulk action option for user actions

This feature allows the addition of custom roles to limit what the admin can see and control. The new custom role limits the ability to select bulk actions such as log off, disconnect, or message. This control is necessary to prevent unintentional or malicious mass actions on users.

You can now edit roles to limit bulk action permissions using the following steps:

1. Sign in to Citrix Cloud.
2. Navigate to **Role** and select the **Perform bulk actions is not enabled** role.
3. Click the three dots and select **Edit**.
4. Go to **Director > Manage** and select the **Perform bulk actions for machines power actions, maintenance mode operations, and session management** check box.
5. Ensure the following roles are also selected:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Enable/disable maintenance mode of a machine via Machine Catalog Membership**
- **Enable/disable maintenance mode on desktop via Machine Catalog Membership**
- **Perform power operations on Windows Desktop machines via Machine Catalog Membership**
- **Perform power operations on Windows Server machines via Machine Catalog Membership**

If the options in step 5 are selected, the user can perform a single action. To perform bulk actions, the option in step 4 and the options in step 5 have to be selected.

Resolve application failures

In the **Activity Manager** view, click the **Applications** tab. You can view all the applications on all machines to which this user has access, including local and hosted applications for the currently connected machine, and the status of each.

The list includes only those applications that were launched within the session.

For Multi-session OS machines and Single session OS machines, applications are listed for each disconnected session. If the user is not connected, no applications are displayed.

ACTION	DESCRIPTION
End the application that is not responding	Choose the application that is not responding and click **End Application**. Once the application is terminated, ask the user to launch it again.
End processes that are not responding	If you have the required permission, click the **Processes** tab. Select a process that is related to the application or using a high amount of CPU resources or memory, and click **End Process**. However, if you do not have the required permission to terminate the process, attempting to end a process fails.
Restart the user's machine	For Single session OS machines only, for the selected session, click **Restart**. Alternatively, from the Machine Details view, use the power controls to restart or shut down the machine. Instruct the user to log on again so that you can recheck the application. For Multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION
	OS machines, the restart option is not available. Instead, log off from the user and let the user log on again.
Put the machine into maintenance mode	If the machine's image needs maintenance, such as a patch or other updates, put the machine into maintenance mode. From the Machine Details view, click **Details** and turn on the maintenance mode option. Escalate to the appropriate administrator.

Disable the visibility of running applications

By default, the Activity Manager displays a list of all running applications for a user's session. This information can be viewed by all administrators that have access to the Activity Manager feature. For Delegated Administrator roles, this includes Full Administrator, delivery group Administrator, and Help Desk Administrator.

To protect the privacy of users and the applications that they are running, you can disable the Applications tab to list running applications. To do this, on the VDA, modify the registry key at HKEY_LOCAL_MACHINE\\Software\\Citrix\\Director\\TaskManagerDataDisplayed. By default, the key is set to 1. Change the value to 0, which means the information is not collected from the VDA and hence not displayed in the Activity Manager.

WARNING:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Restore desktop connections

From Monitor, check the user's connection status for the current machine in the user title bar.

If the desktop connection failed, the error that caused failure is displayed and can help you decide how to troubleshoot.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACTION	DESCRIPTION
Ensure that the machine is not in maintenance mode	On the User Details page, make sure maintenance mode is turned off.
Restart the user's machine	Select the machine and click **Restart**. Use this option if the user's machine is unresponsive or unable to connect, such as when the machine is using an unusually high amount of CPU resources, which can make the CPU unusable.

Restore sessions

If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the server.

In the User Details view, troubleshoot session failures in the **Session Details** panel. You can view the details of the current session, indicated by the session ID.

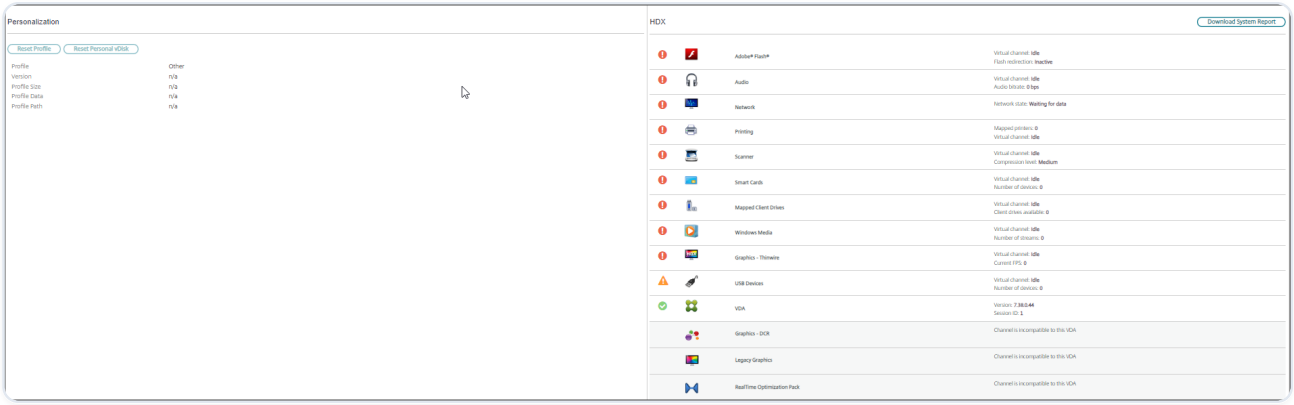
ACTION	DESCRIPTION
End applications or processes that are not responding	Click the **Applications** tab. Select any application that is not responding and click **End Application**. Similarly, select any corresponding process that is not responding and click **End Process**. Also, end processes that are consuming an unusually high amount of memory or CPU resources, which can make the CPU unusable.
Disconnect the Windows session	Click **Session Control** and then select **Disconnect**. This option is available only for brokered Multi-session OS machines. For non-brokered sessions, the option is disabled.
Log off the user from the session	Click **Session Control** and then select **Log Off**.

To test the session, the user can attempt to log back on to it. You can also shadow the user to more closely monitor this session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Run HDX™ channel system reports

In the **User Details** view, check the status of the HDX channels on the user's machine in the HDX panel. This panel is available only if the user machine is connected using HDX.



If a message appears indicating that the information is not currently available, wait for one minute for the page to refresh, or select the **Refresh** button. HDX data takes a little longer to update than other data.

Click an error or warning icon for more information.

Tip:

> You can view information about other channels in the same dialog box by clicking the left and right arrows in the left corner of the title bar.

HDX channel system reports are used mainly by Citrix Support to troubleshoot further. To do this, in the HDX panel, click **Download System Report**.

Reset a user profile

CAUTION:

When a profile is reset, although the user's folders and files are saved and copied to the new profile, most user profile data is deleted (for example, the registry is reset and application settings might be deleted).

1. From Monitor, search for the user whose profile you want to reset and select this user's session.
2. Click **Reset Profile**.
3. Instruct the user to log off from all sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Instruct the user to log back on. The folders and files that were saved from the user's profile are copied to the new profile.

   IMPORTANT:

   If the user has profiles on multiple platforms (such as Windows 8 and Windows 7), instruct the user to log back on first to the same desktop or app that the user reported as a problem. This ensures that the correct profile is reset. For a Citrix® user profile, the profile is already reset by the time the user's desktop appears. For a Microsoft roaming profile, the folder restoration might still be in progress for a brief time. The user must stay logged on until the restoration is complete.

The preceding steps assume you are using Citrix Virtual Desktops™ (Desktop VDA). If you are using Citrix Virtual Desktops (Server VDA) you need to be logged on to perform the profile reset. The user then needs to log off, and log back on to complete the profile reset.

If the profile is not successfully reset (for example, the user cannot successfully log back on to the machine or some of the files are missing), you must manually restore the original profile.

The folders (and their files) from the user's profile are saved and copied to the new profile. They are copied in the listed order:

- Desktop
- Cookies
- Favorites
- Documents
- Pictures
- Music
- Videos

NOTE:

In Windows 8 and later, cookies are not copied when profiles are reset.

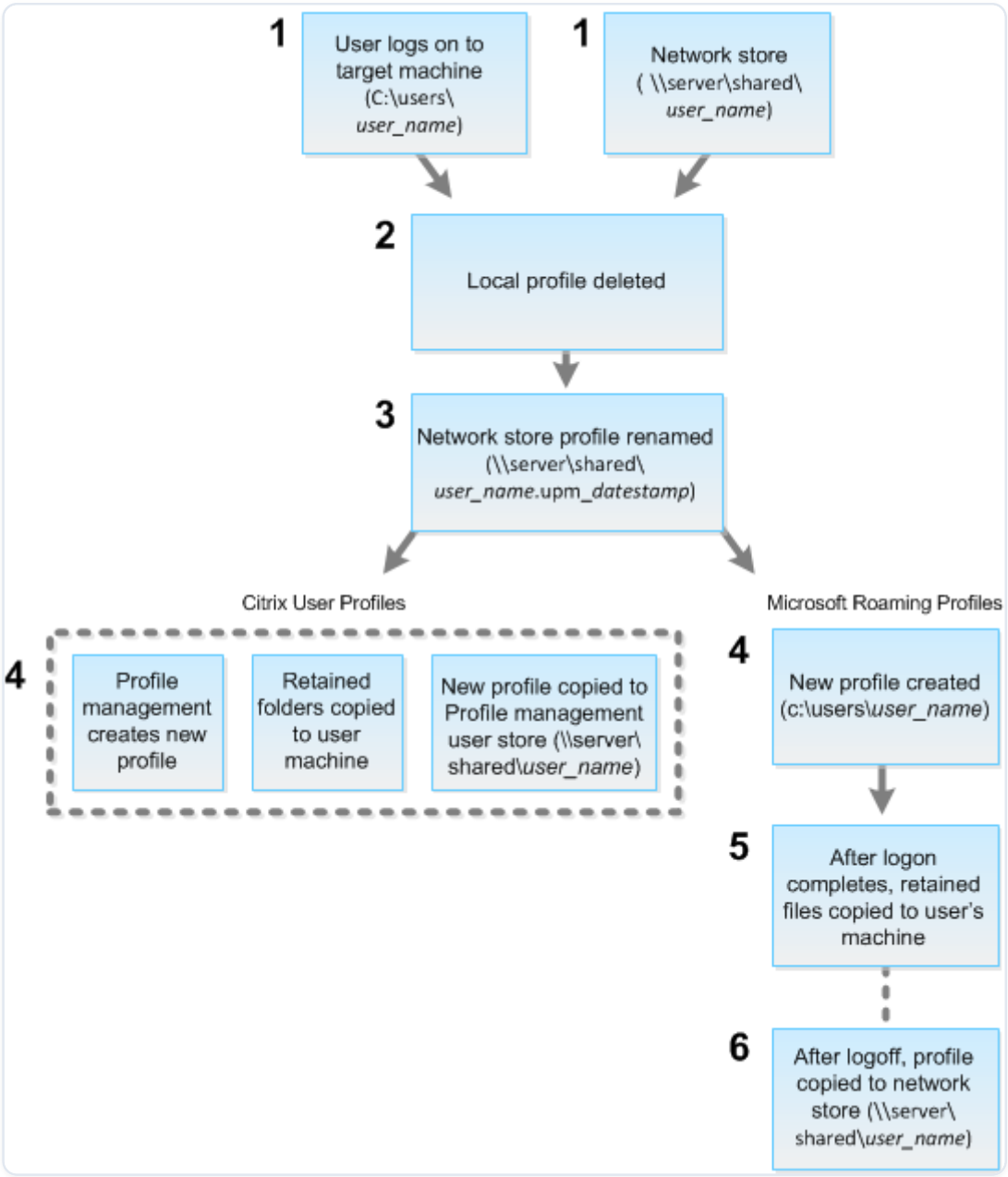
How reset profiles are processed

Any Citrix user profile or Microsoft roaming profile can be reset. After the user logs off and you select the reset command (either in Monitor or using the PowerShell SDK), Monitor first identifies

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the user profile in use and issues an appropriate reset command. Monitor receives the information through Profile Management, including information about the profile size, type, and logon timings.

This diagram illustrates the process following the user log on, when a user profile is reset.



The reset command issued by Monitor specifies the profile type. The Profile Management service then attempts to reset a profile of that type and looks for the appropriate network share (user store). If Profile Management processes the user, but receives a roaming profile command, it is rejected (or the opposite way).

1. If a local profile is present, it is deleted.
2. The network profile is renamed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. The next action depends on whether the profile being reset is a Citrix user profile or a Microsoft roaming profile.

   For Citrix user profiles, the new profile is created using the Profile Management import rules, and the folders are copied back to the network profile, and the user can log on normally. If a roaming profile is used for the reset, any registry settings in the roaming profile are preserved in the reset profile. You can configure Profile management so that a template profile overrides the roaming profile, if necessary.

   For Microsoft roaming profiles, Windows creates a new profile, and when the user logs on, the folders are copied back to the user device. When the user logs off again, the new profile is copied to the network store.

To manually restore a profile after a failed reset

1. Instruct the user to log off from all sessions.
2. Delete the local profile if one exists.
3. Locate the archived folder on the network share that contains the date and time appended to the folder name, the folder with a .upm_datestamp extension.
4. Delete the current profile name. That is, the one without the upm_datestamp extension.
5. Rename the archived folder using the original profile name. That is, remove the date and time extension. You have returned the profile to its original, pre-reset state.

Record sessions

You can record ICA® sessions using the Session Recording controls from the **User Details** and **Machine Details** screen in Director. This feature is available for customers on **Premium** sites.

Dynamic Session Recording

You can record the current active session using the Session Recording controls from the **User Details** screen. For more information about Dynamic Session Recording, see the Session Recording service article.

Policy based Session Recording

To configure Policy-based Session Recording on Director using the DirectorConfig tool, see the **Configure Director to use the Session Recording Server** section in Configure session recording policies. The Session Recording controls are available in Director only if the logged-in user has the permission to modify the Session Recording policies. This permission can be set on the Session Recording Authorization console as described in Authorize users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

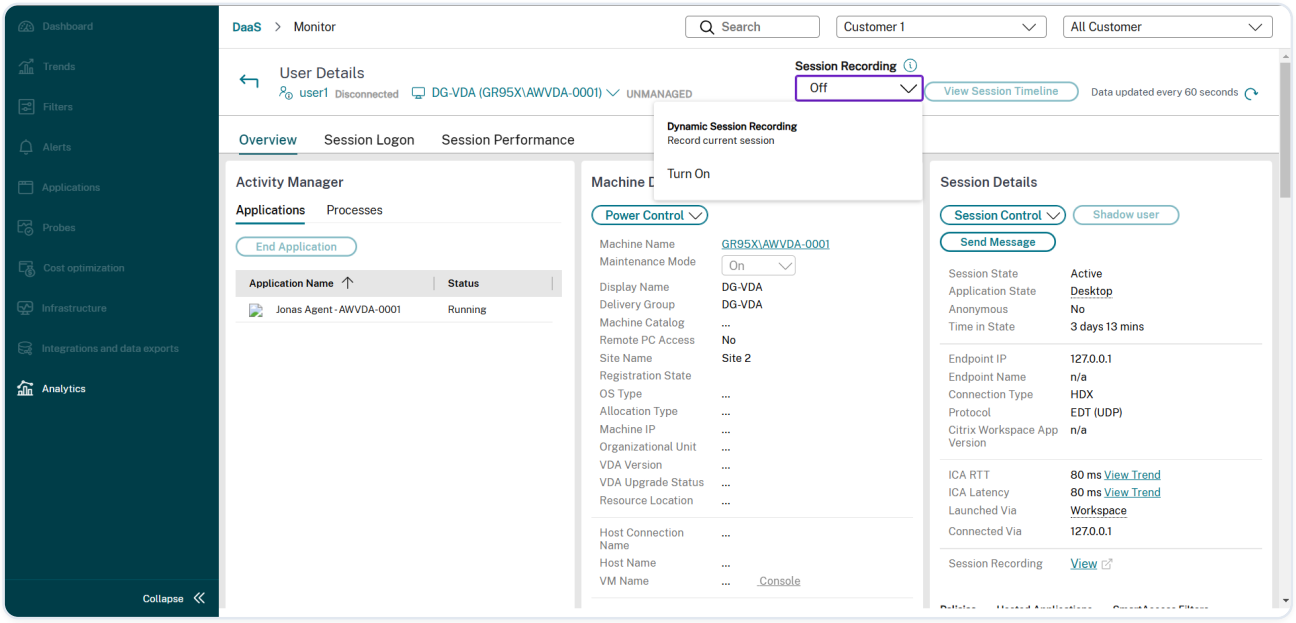
Changes made to the Session Recording settings through Director or the Session Recording Policy console take effect starting from the subsequent ICA session.

Session Recording controls in Director

You can use the **User Details** > **Session Recording** actions to record the current or subsequent sessions.

- Turn ON Dynamic Session Recording - the current session is recorded.
- Turn ON (with notification) - the subsequent sessions are recorded and the user is notified about the session being recorded on logging on to the ICA session.
- Turn ON (without notification) - the subsequent sessions are recorded and the session is recorded silently without notifying the user.
- Turn OFF - disable recording of sessions for the user.

The **Policies** Panel displays the name of the active Session Recording policy.



The **Machine Details** panel displays the status of the Session Recording policy for the machine.

PLAY BACK LIVE AND RECORDED SESSIONS

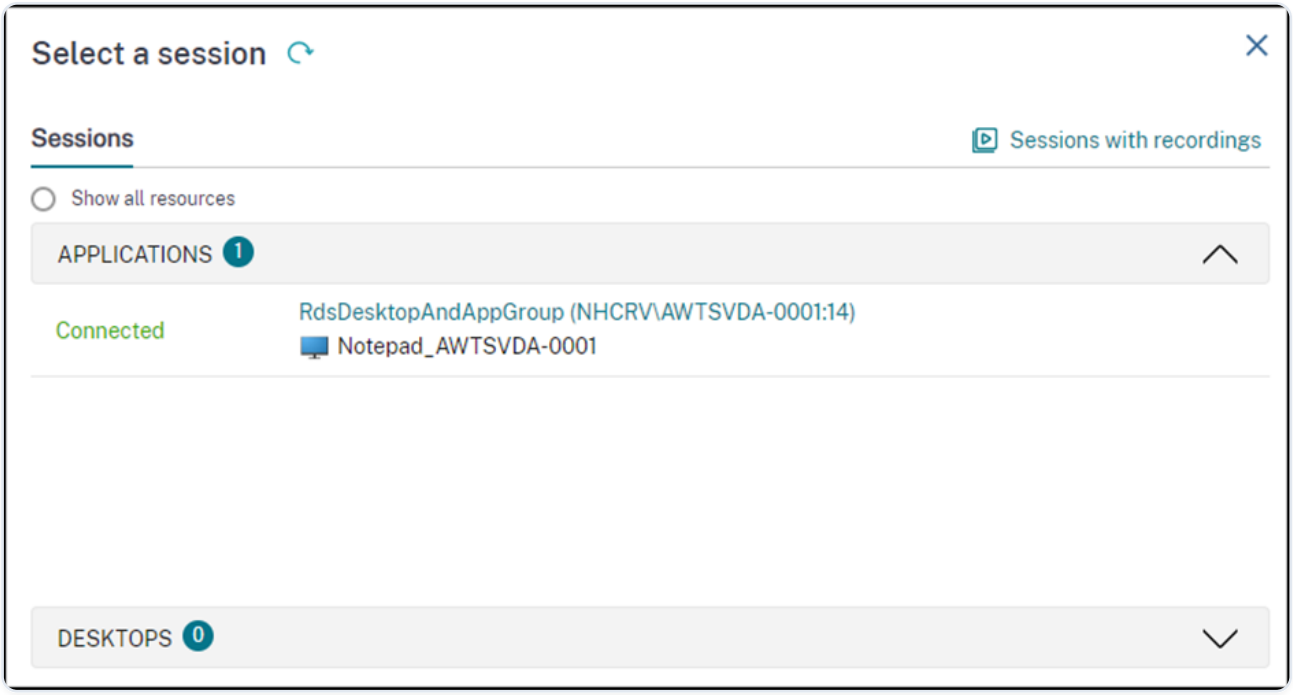
You can play back recorded and live user sessions to understand the issues encountered by the user. Ready access to recordings and session related metrics within the Director console eliminates the requirement of searching for the recordings across multiple session recording servers or looking for third-party apps to view the recordings. It helps corelate the issues discovered in the recordings with the performance metrics.

This feature requires the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

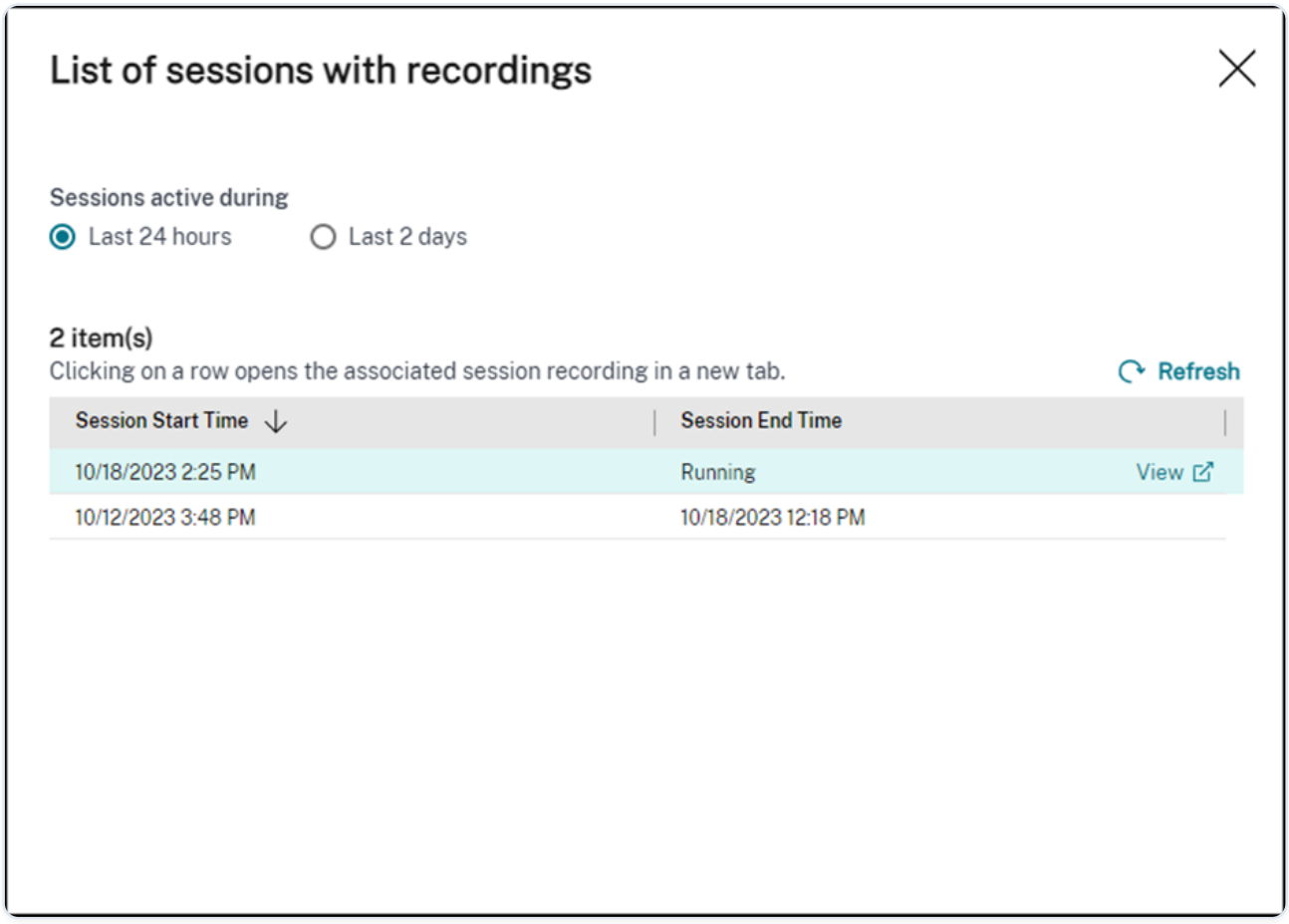
- VDA and the Session Recording servers are on version 2308 or later.
- Delivery Controller™ and Director are on version 2311 or later.

Director stores session recordings in a centralized repository. The list of recordings belonging to the user are displayed on clicking the **Session Selector** modal > **Sessions with recordings** link.



You can choose to view recordings of sessions that were active during the last 24 hours or the last 2 days. Live recordings of currently active sessions are marked with **Session End Time** as **Running**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click the **View** link to play back the recording on a new tab using the Citrix Session Recording playback server.

Troubleshoot machines

NOTE:

Citrix Health Assistant is a tool to troubleshoot configuration issues in unregistered VDAs. The tool automates a number of health checks to identify possible root causes for VDA registration failures and issues in session launch and time zone redirection configuration. The Knowledge Center article, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch contains the **Citrix Health Assistant** tool download and usage instructions.

The **Filters \> Machines** view in the Monitor tab displays the machines configured in the site. The Multi-session OS Machines tab includes the load evaluator index, which indicates the distribution of performance counters and tooltips of the session count if you hover over the link.

Click the **Failure Reason** column of a failed machine to get a detailed description of the failure and actions recommended to troubleshoot the failure. The failure reasons and the recommended

© 1997–2026 Citrix Systems, Inc. All rights reserved.

actions for machine and connection failures are available in the Citrix Director Failure Reasons Troubleshooting Guide.

Click the machine name link to go to the **Machine Details** page.

The Machine Details page lists the machine details, infrastructure details, and details of the hotfixes applied on the machine.

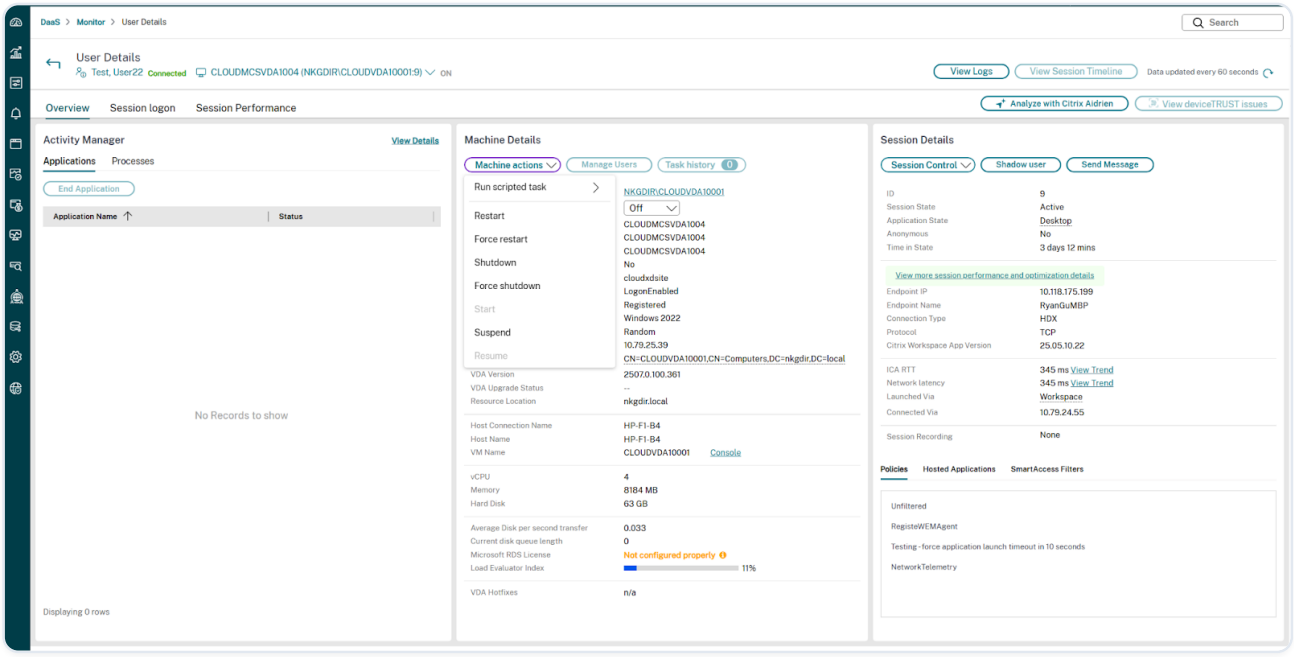
Support for HDX™ Plus for Windows 365 Cloud PCs and Azure Virtual Desktops:

NOTE:

For HDX Plus for Windows 365 Cloud PCs, only the Restart and Force Restart Power Control options are available. For Azure Virtual Desktops (AVD) all Power Control options are available.

You can view the available Power Control options using one of the following methods:

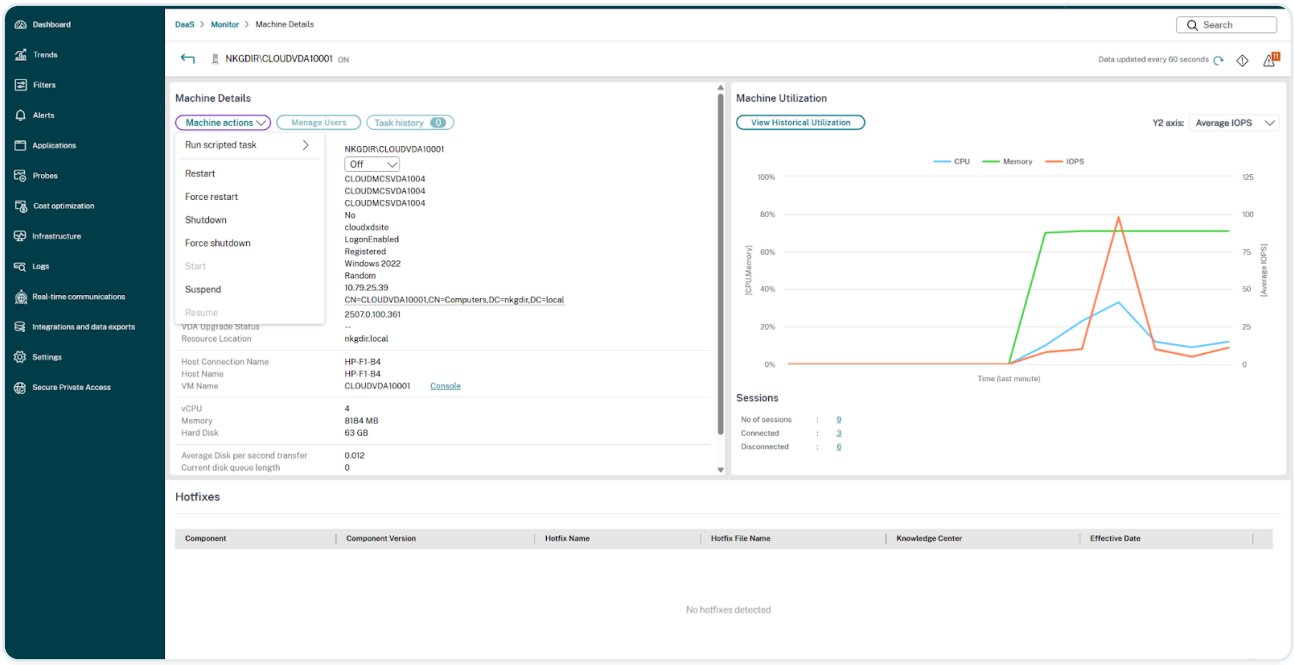
Click **Filters** > **Sessions** > **Machine Details** > **Machine actions** drop-down list and select an option to assign the required power control or scripted task option for a machine.



Or,

Click **Filters** > **Machine** > **Machine Details** > **Machine actions** drop-down list and select an option to assign the required power control or scripted task option for a machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

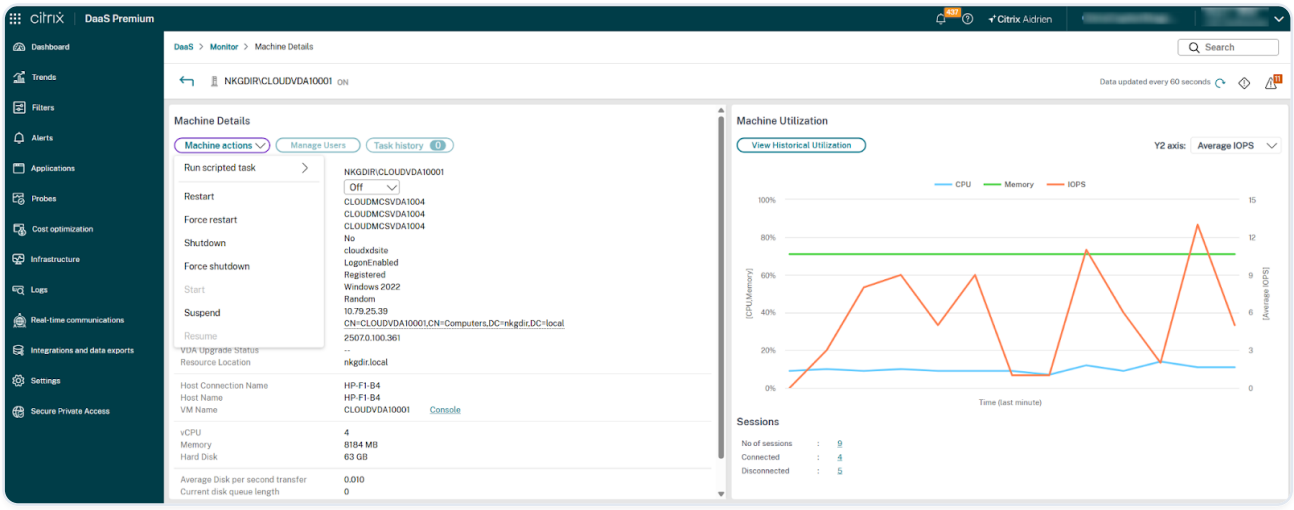
- Run Scripted Task is supported only when the WEM(Workspace Environment Management) service is provisioned and the WEM agent on the VDA is installed and registered with the WEM service.
- Task History shows only the current user's Scripted Task executions within the last 24 hours.

Machine-based real-time resource utilization

The **Machine Utilization** panel displays graphs showing real-time utilization of CPU and memory. In addition, disk and GPU monitoring graphs are available for sites with VDA versions 7.14 and later.

Disk monitoring graphs, average IOPS, and disk latency are important performance measurements that help you monitor and troubleshoot issues related to VDA disks. The Average IOPS graph displays the average number of reads and writes to a disk. Select **Disk Latency** to see a graph of the delay between a request for data and its return from the disk, measured in milliseconds.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



GPU UTILIZATION

Select **GPU Utilization** to see the percentage utilization of the GPU, the GPU memory, and of the Encoder and the Decoder to troubleshoot GPU-related issues on multi-session and single-session OS VDAs.

Supported GPU versions:

- NVIDIA Tesla M60 GPUs running Display Driver version 369.17 or later. For more information, see NVIDIA vGPU Software.
- AMD Radeon Instinct MI25 GPUs and AMD EPYC 7V12(Rome) CPUs. For more information, see AMD Drivers and Support.

Drivers:

The appropriate drivers or extensions must be installed on the VDAs.

- For NVIDIA GPUs, install GRID drivers manually or via extensions. For more information, see NVIDIA vGPU Software.
  - Note that for NVIDIA, only GRID drivers are supported. CUDA drivers do not work with the NVadsA10 v5-series and are not supported.
  - For a sample process to install Nvidia Grid GPU drivers via extensions on Azure based machines, see NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
  - For a sample process to install Nvidia Grid GPU drivers manually, see Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.
- For AMD GPUs, install AMD graphics drivers manually or via extensions. For more information, see AMD Drivers and Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For a sample process to install AMD GPU drivers via extensions on Azure based machines, see AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
- For a sample process to install AMD GPU drivers manually on Azure machines, see Install AMD GPU drivers on N-series VMs running Windows.

Usage Notes:

- The GPU Utilization graphs are available only for VDAs running 64-bit Windows.
- The AMD GPU Utilization graphs are available only for VDAs running Citrix Virtual Apps and Desktops™ 7 2212 or later.
- The VDAs must have HDX 3D Pro enabled to provide GPU acceleration. For more information, see GPU acceleration for Windows Single-session OS and GPU acceleration for Windows Multi-session OS.
- When a VDA accesses more than one GPU, the utilization graph displays the average of the GPU metrics collected from the individual GPUs. The GPU metrics are collected for the entire VDA and not for individual processes.
- For AMD, encoder and decoder usage are not supported separately. Any encoding/ decoding workload using the GPU will be reported as the general 3D load on GPU usage.
- Ensure that you install the NVIDIA WMI during installation. This window is available only during manual installation.
- If drivers are installed but Director does not detect GPU
  - Check Task Manager. If drivers are installed properly, the GPU should show up in Task Manager.
  - Check if the machine is registered. Sometimes machines may take some time to be detected as online.
- If the GPU usage shows no activity in Director, make sure that the workload you are running is using the GPU. For graphics workloads, this can be enabled from Settings > System > Display > Graphics Settings > Choose the app to set preference. Make sure to turn on High Performance. Sometimes, Windows defaults to using the CPU for graphics workloads when this is set to system default or power saving, based on other settings.
- The data is updated every minute and the data visualization starts within a minute of selecting **GPU Utilization**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

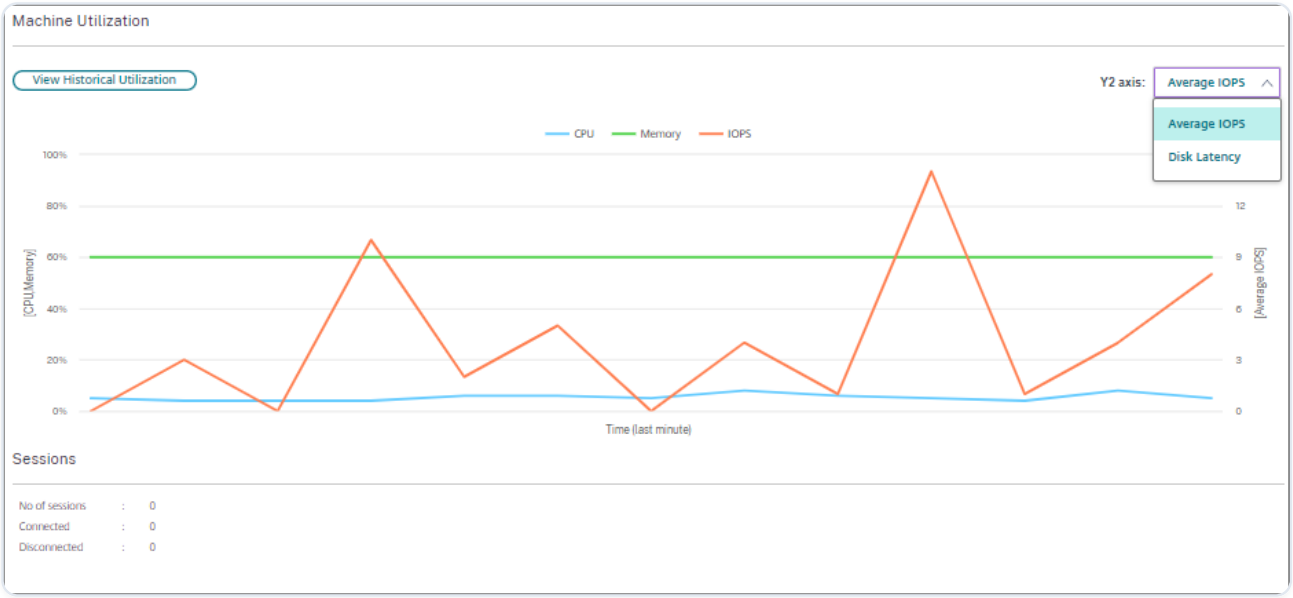
Machine-based historical resource utilization

In the **Machine Utilization** panel, click **View Historical Utilization** to view the historical usage of resources on the selected machine. The utilization graphs include critical performance counters of CPU, memory, peak concurrent sessions, average IOPS, and disk latency.

NOTE:

The Monitoring policy setting, **Enable Process Monitoring**, must be set to Allowed to collect, and display data in the Top 10 Processes table on the Historic Machine Utilization page. The collection is prohibited by default.

The CPU and memory utilization, average IOPS, and disk latency data is collected by default. You can disable the collection by using the **Enable Resource Monitoring** policy setting.



1. From the **Machine Utilization** panel in the **Machine Details** view, select **View Historical Utilization**.
2. In the **Historical Machine Utilization** page, set **Time Period** to view usage for the last 2 hours, 24 hours, 7 days, month, or year.

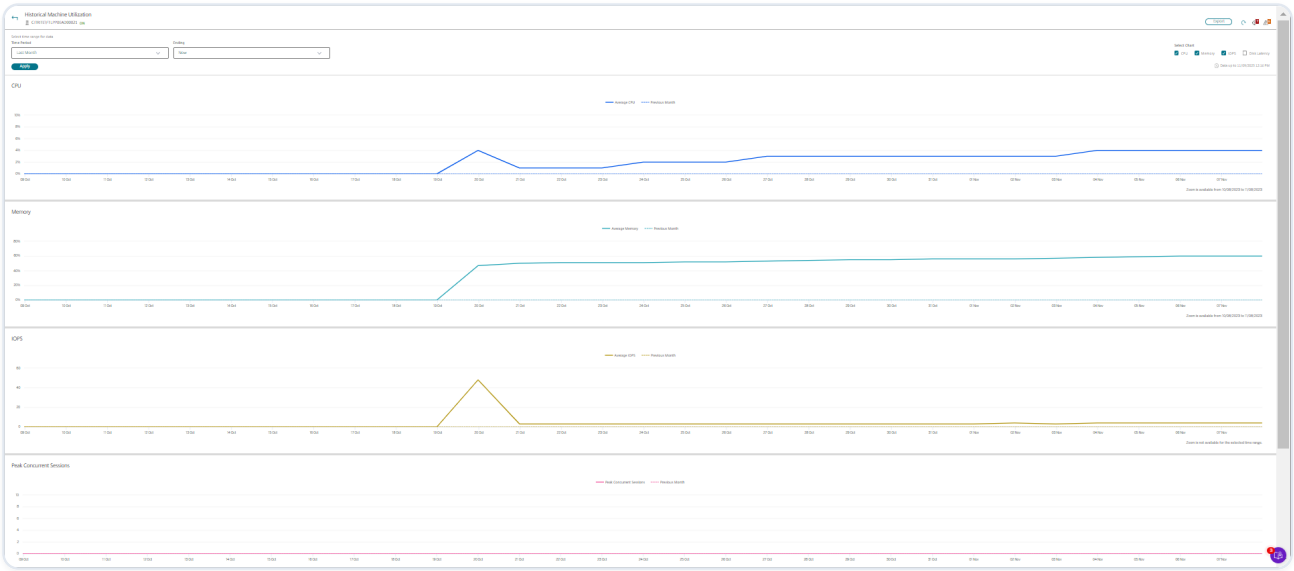
   NOTE:

   Average IOPS and disk latency usage data are available only for the last 24 hours, month, and year ending now. Custom end time is not supported.

3. Click **Apply** and select the required graphs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Hover over different sections of the graph to view more information for the selected time period.



For example, if you select **Last 2 hours**, the baseline period is the 2 hours prior to the selected time range. View the CPU, memory, and session trend over the last 2 hours and the baseline time. If you select **Last month**, the baseline period is the previous month. Select to view the Average IOPS and disk latency over the last month and the baseline time.

1. Click **Export** to export the resource utilization data for the selected period. For more information, see Export reports section in Monitor Deployments.
2. Below the graphs, the table lists the top 10 processes based on CPU or memory utilization. You can sort by any of the columns, which show Application Name, User Name, Session ID, Average CPU, Peak CPU, Average Memory, and Peak Memory over the selected time range. The IOPS and Disk Latency columns cannot be sorted.

   NOTE:

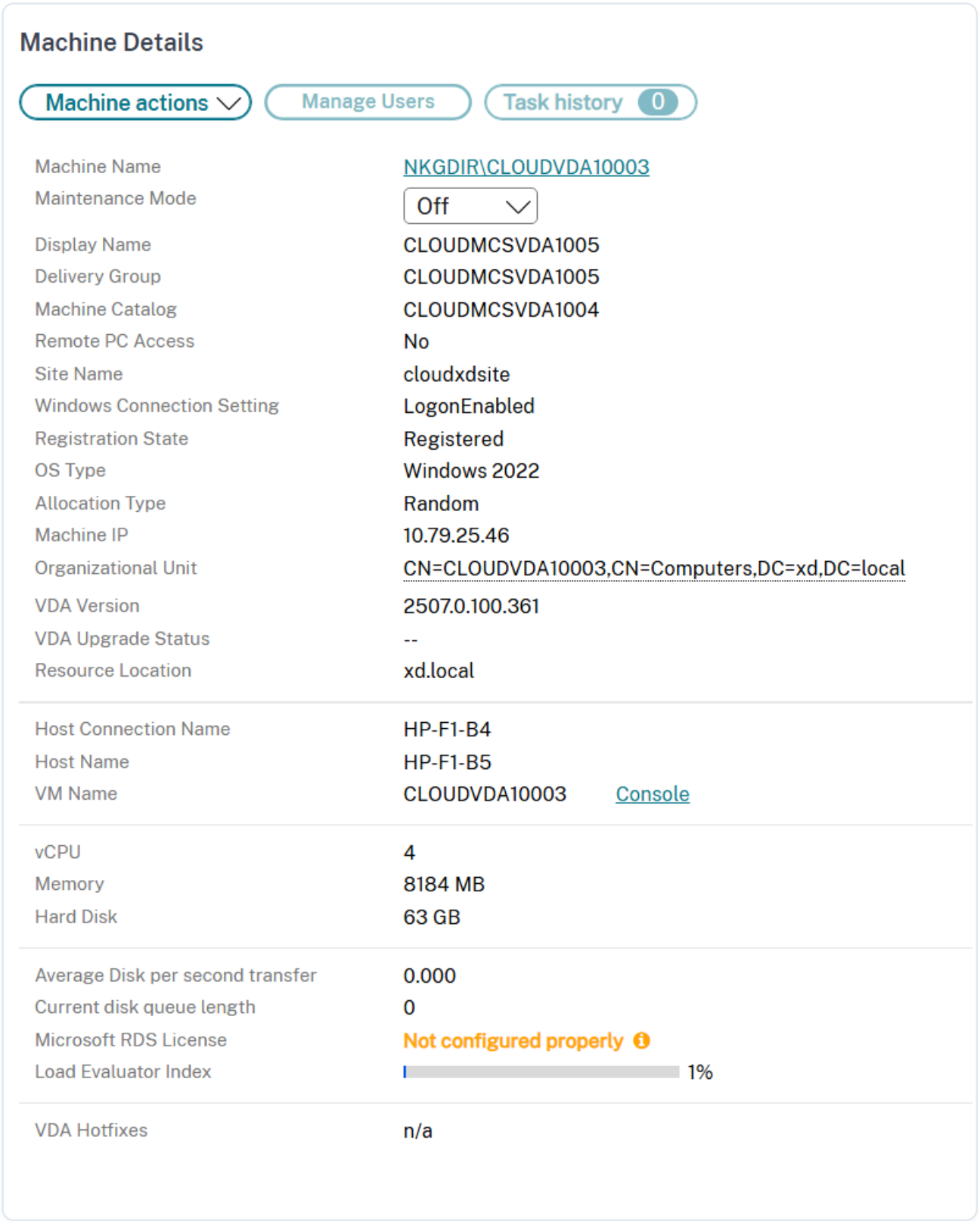
   - The session ID for system processes is displayed as "0000".
   - If a site that belongs to the Citrix Cloud™ Japan or the Citrix Cloud Government plane contains more than 5000 machines, process data is available for up to 2000 machines only. The Process Monitoring policy must be enabled on these machines.

3. To view the historical trend on the resource consumption of a particular process, drill into any of the Top 10 processes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Machine Console access

You can access the consoles of Desktop and Multi-session OS machines hosted on XenServer Version 7.3 and later directly from Monitor. This way, you don't require XenCenter to troubleshoot issues on XenServer hosted VDAs. For this feature to be available, the XenServer hosting the machine must be of Version 7.3 or later and must be accessible from the Monitor.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

To troubleshoot a machine, click the **Console** link in the corresponding Machine Details panel. After authentication of the host credentials you provide, the machine console opens in a separate tab using noVNC, a web-based VNC client. You now have keyboard and mouse access the console.

NOTE:

- This feature is not supported on Internet Explorer 11.
- If the mouse pointer on the machine console is misaligned, see CTX230727 for steps to fix the issue.
- Console access is launched on a new tab, ensure that your browser settings allow pop-ups.
- For security reasons, Citrix® recommends that you install SSL certificates on your browser.

Inspect machines with recent power actions

You can now inspect machines with the status of the success and failed power actions. This feature helps you to analyze the following:

- Power on failure which causes user issues
- Power off failure which increases cost

NOTE:

Data is available only for the power-managed machine. Data isn't available for the power actions taken before the feature was supported.

You can view the power action status of the machines using the following ways:

From **Filters** -> **Machines** tab. In this case, by default the **Power Action Time** and the **Power Action Result** columns are visible. You can also select the columns that you want to visible.

From **Cost Optimization** tab. In this case, the default filter is **Power Action Triggered By** is set to *Autoscale*™ and the **Power Action Result** is set to *Failed*.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With this feature, you can view the details of the power action controls. For example, you can view who triggered the action, which action changed the power state, the reason for failure, and the time when the action is completed. You can also export these details.

The following filters are added to view the power action status:

FILTER	DESCRIPTION
Power Action Result	Displays the result of the power action. The possible filter values are success and failed.
Power Action Triggered By	Displays who or what triggered the power action. The possible filter values are the following
	• Autoscale - This value appears when a power action is triggered by the following
	• When admin shut-down a VM to clean the VM's OS disk back to its initial state
	• When a VM is shut down or suspended based on the set policies
	• When a VM is made available based on the pool size or buffer size configuration
	• Admin - This value appears when a power action is triggered by an admin. The possible examples are when admin requests for turn off, turn on, suspend, resume, restart, or reboot a VM.
	• User - This value appears when a power action is triggered by a user. The

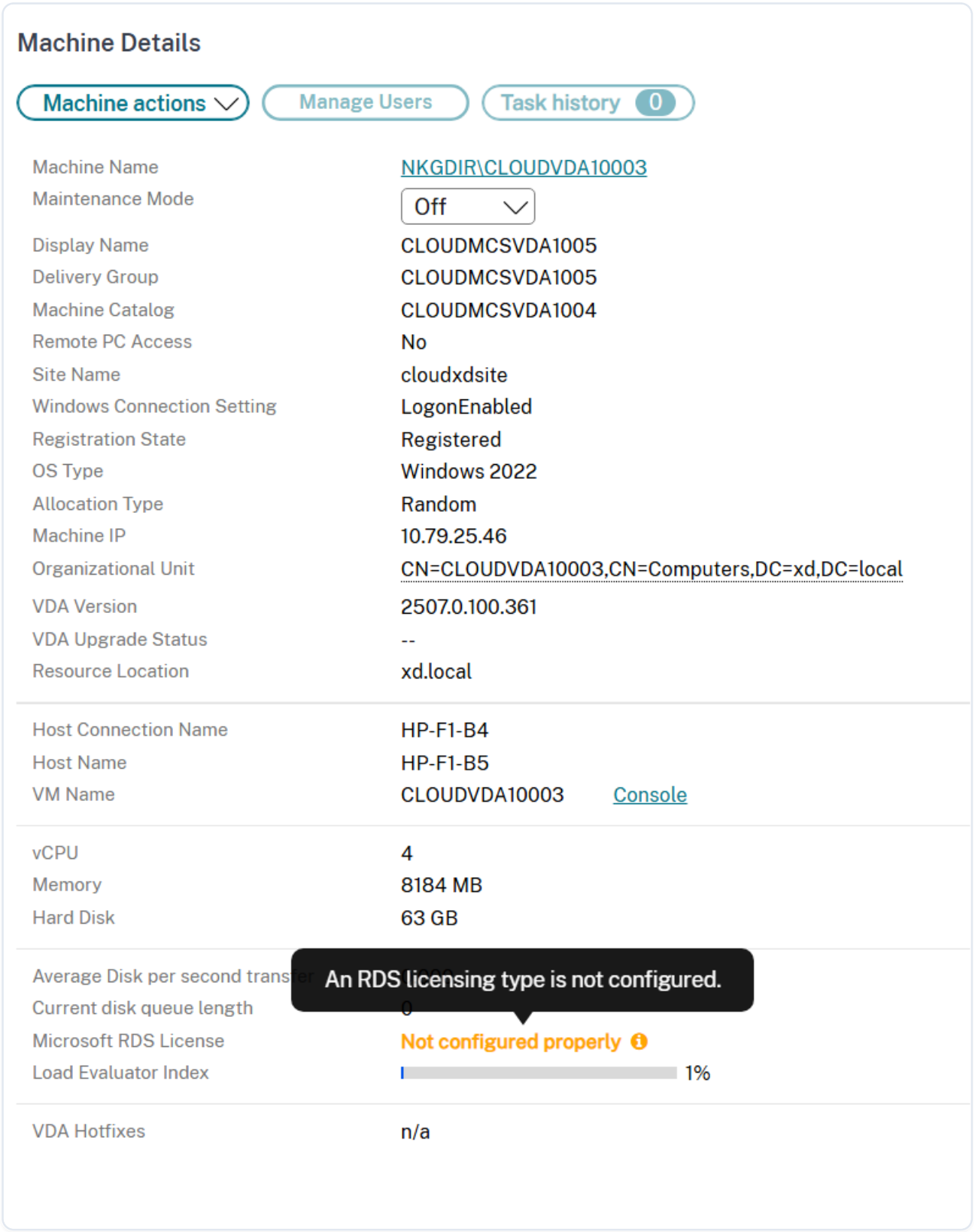
© 1997–2026 Citrix Systems, Inc. All rights reserved.

FILTER	DESCRIPTION
	examples are when a user resets, turn on, or resume work on the VM. • Others - This value appears when power action is triggered by scheduled and by unknown reasons.
Last Power Action	Displays the exact power action happened on the machine such as power-on, power off, shut down, restart, reset, resume, and so on
Power Action Time	The time when the power action is completed. The possible filter values are last minute, last 5 minutes, last 30 minutes, last hour, today, last 24 hours, and yesterday.
Power Action Failure Reason	Displays the reason for failure. The possible filter values are hypervisor reported failure, hypervisor rate limit exceeded, unknown error, and none. If there is a successful action, it shows "None".

Microsoft RDS license health

You can view the status of Microsoft RDS license in the Machine Details panel in the **Machine Details** and the **User Details** page for Multi-session OS machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



One of the following messages is displayed:

- License available
- Not configured properly (warning)
- License error (error)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Incompatible VDA version (error)

NOTE:

The Microsoft RDS license health status for machines under grace period with valid license displays a **License available** message in green. Renew your license before they expire.

For warning and error messages, hover over the info icon to view additional information as given in the following table.

MESSAGE TYPE	MESSAGES IN MONITOR
Error	Available for VDAs version 7.16 and later.
Error	New RDS connections are not allowed.
Error	Microsoft RDS license has exceeded its grace period.
Error	A License Server is not configured for the required OS level with the Per Device Client Access licensing type.
Error	The configured License Server is incompatible with the RDS Host OS level with the Per Device Client Access licensing type.
Warning	Personal Terminal Server is not a valid RDS licensing type in a Citrix Virtual Apps and Desktops deployment.
Warning	Remote Desktop for Administration is not a valid licensing type in a Citrix Virtual Apps and Desktops deployment.
Warning	An RDS licensing type is not configured.
Warning	The Domain Controller or License Server is unreachable with the Per User Client Access RDS licensing type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

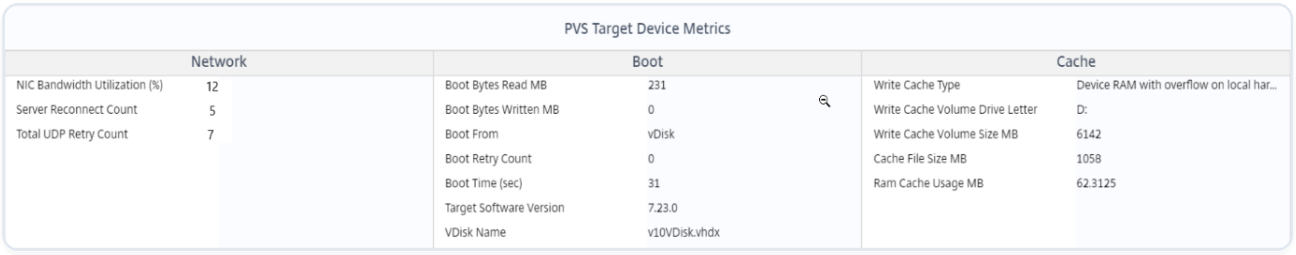
MESSAGE TYPE	MESSAGES IN MONITOR
Warning	With the Per Device Client Access licensing type, the Client Device license could not be determined since the license server for the required OS level is unreachable.

NOTE:

This feature is applicable only for Microsoft RDS CAL (Client Access License).

PVS target device metrics

You can view the status of PVS target devices for single-session and multi-session OS machines on the **Machine Details** page in Monitor. Several metrics for **Network**, **Boot**, and **Cache** are available on this panel. These metrics help you monitor and troubleshoot PVS target devices to ensure that they are up and running.



Network:

- Network Bandwidth Utilization: Average bandwidth utilization across all NICs.
- Server Reconnect Count: Number of times the server has reconnected due to network issues or server rebalancing or shutdowns and restarts of the Citrix Provisioning™ Stream Service.
- Total UDP Retry Count: Number of times the provisioning target device has tried to reconnect to the provisioning server using UDP. This metric helps you to know if there are any network issues in the Citrix Provisioning Stream Service (for example, bad switch configurations).

Boot:

- Boot Bytes Read MB: Bytes read while booting.
- Boot Byes Written MB: Bytes written while booting.
- Boot From: Boot medium (vDisk, local disk, and so on).
- Boot Retry Count: Number of retries to boot the machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Boot Time: Time taken to boot the machine, in seconds. By default, there is a 5 second delay between retries. If this delay grows into double digits, there is a significant increase in boot time. Check your provisioning configuration to resolve this issue.
- Target Software Version: Version of the Provisioning target device software.
- vDisk Name: vDisk from which the Provisioning target device is booting.

Cache:

- Write Cache Type: vDisk can be set to different types of cache. For more information, see Knowledge Center article CTX119469.
- Write Cache Volume Drive Letter: Drive letter for write cache types involving drives.
- Write Cache Volume Size MB: Total configured volume size for write cache.
- Cache File Size MB: Current cache file size (cache on device RAM with overflow on hard disk).
- Ram Cache Usage MB: Current RAM cache size (cache on device RAM with overflow on hard disk). Use Overflow to disk only if necessary. This metric is useful when setting or optimizing the proper size of RAM cache.

For more information, see Using the Status Tray on a target device.

Provisioning target device metrics is available only on:

- Provisioning machines.
- Provisioning target device version 7.19 and later.
- VDA version 2003 and later.

NOTE:

Metrics for Server Reconnect Count and UDP Retry Count are available only for Provisioning target version 1912 CU2 and later.

Infrastructure monitoring

Citrix Monitor now offers visibility into the operational health of Citrix DaaS™ components. This feature helps you to easily identify, troubleshoot, and resolve issues related to your infrastructure. Currently, the health of the components are monitored:

- Cloud Connector
- Citrix Provisioning™ Service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- StoreFront™
- Connector Appliance

To support this feature, a new Windows executable named `citrixinframonitor.msi` is introduced for Citrix components. This helps with the collection and transmission of relevant health metrics from Provisioning Service or StoreFront servers to Monitor. However, `citrixinframonitor.msi` is not required for monitoring Cloud Connector. Cloud connectors are automatically onboarded when a connection between Citrix Cloud and your resource locations is established.

This feature helps you to get critical monitoring data sets and proactive alerts regarding the Cloud Connector, Provisioning Service, and StoreFront server's system metrics on a single console in Monitor. Data is collected every five minutes from the monitoring components to ensure the latest information.

This feature aims to enhance operational efficiency by offering proactive monitoring, detailed metrics, and automated alerts, ensuring your Citrix infrastructure runs smoothly and efficiently.

Key features

Real-time monitoring:

- Continuous monitoring of Citrix infrastructure components such as Cloud Connector, Citrix Provisioning (Provisioning Service) servers, StoreFront, and Connector Appliance.
- Dashboard views presenting system health, resource utilization, and relevant performance metrics.

Detailed analysis:

- Provides detailed analysis on the system health metrics such as connectivity status, and service or process status for each component.
- Details on the resource utilization metrics such as CPU, memory, and disk utilization.

Automated alerts and notifications:

- Customizable alert thresholds for various metrics and states with granular scopes.
- Real-time notifications through email and webhooks.

Use-cases

Operational efficiency:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ensures that Citrix admin teams can maintain high availability and performance of their Citrix servers and services. This feature also helps in minimizing downtime by proactively identifying and alerting admins on issues before they impact significant user groups.

Faster ticket resolution:

Monitors key metrics on server health and performance to evaluate the optimal delivery of virtual applications and desktops to users. Use these metrics to diagnose and resolve user complaints related to performance by analyzing associated components.

Prerequisites

- Enusre the prerequisites for Provisioning Service or the prerequisites for StoreFront are met.
- For monitoring Citrix Provisioning:
    - Minimum required version to monitor DB Connectivity and License Server Reachability :
        - 2402 CU1
        - 2407
    - Minimum required version to monitor PXE Service, TFTP Service, and Total Reconnect Count is Citrix Infra Monitor 2411.
- User accounts or permissions required to run Citrix Infrastructure Monitor:
    - User accounts with Windows administrator permissions to install the Citrix Infrastructure Monitor on the endpoint machines.
    - A full administrator user account or a custom role with the following Monitor permissions:
        - Create\Edit\Enable\Delete Alert Policies
        - Create\Edit\Remove Alert Email Server Configuration
        - Dismiss Alerts
        - View Alert Policies
        - View Alerts
        - View Dashboard page
        - View Infrastructure Monitor page
        - To view the **Alerts** page

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- The preceding prerequisite is valid only for Provisioning Service and StoreFront components monitoring.
- If you don't have permission to access the **Alerts** page, the **Manage Alerts** option is disabled on the **Infrastructure Monitoring** page.

To begin using and implementing the **Infrastructure Monitoring** feature in your site, see to the following:

- Getting started with Infrastructure Monitoring
- Set Remote PowerShell SDK
- Manage connections
- Infrastructure dashboard
- Advanced alert policies
- Infrastructure policies

Getting started with Infrastructure Monitoring

NOTE:

The following two steps are valid only for Provisioning Service and StoreFront™ components monitoring.

Step 1: Installation of Citrix Infrastructure Monitor

Perform the following steps to complete the installation on the target component to establish connection for secure data collection.

Step 1.1: Identify the target components

Identify the target components such as Provisioning Service or StoreFront servers which need to be monitored.

Step 1.2 Download Citrix Infrastructure Monitor

You can download `CitrixInfraMonitor.msi` from the Citrix downloads page on the target server identified in Step 1.1.

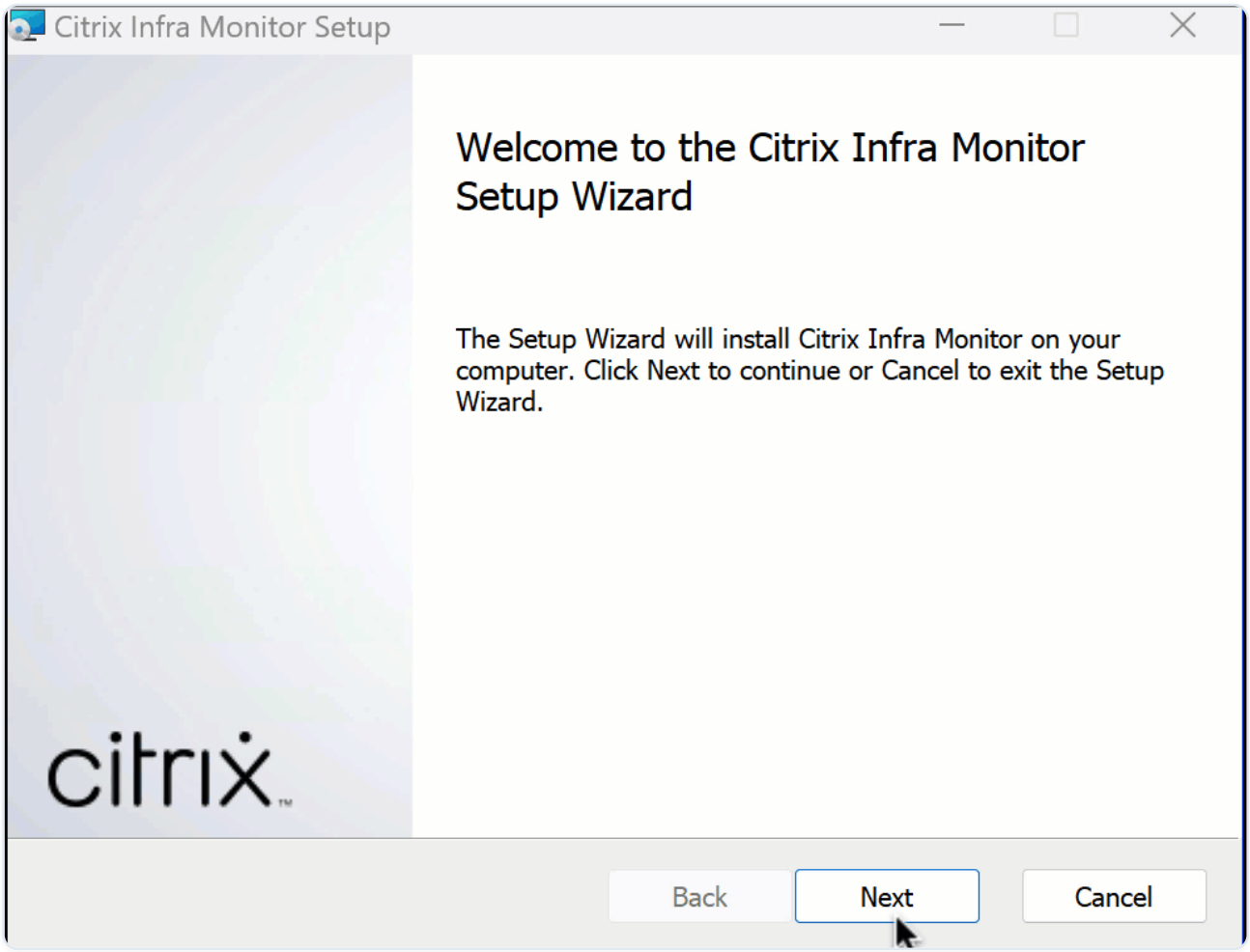
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1.3: Run Citrix Infrastructure Monitor

Run the `CitrixInfraMonitor.msi` installer on the target component by following the instructions in the installation wizard.

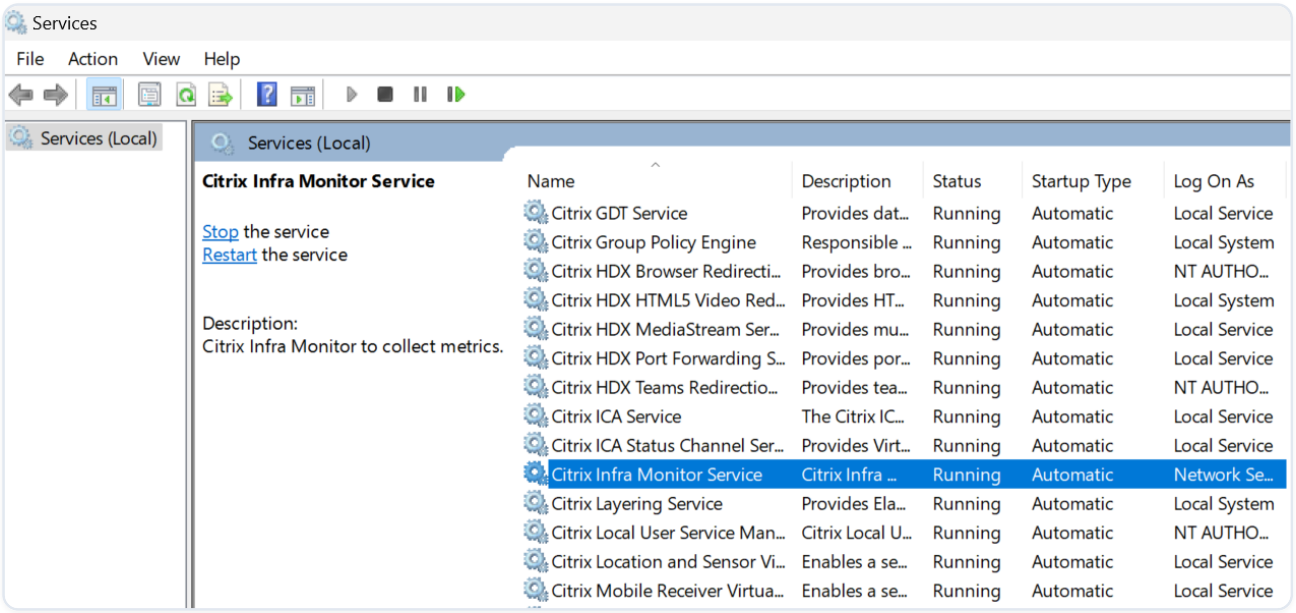
NOTE:

Users with administrative privileges can install and configure Citrix Infrastructure Monitor on the target component.



Once the installation is successful, you can view the Citrix Infrastructure Monitor Service in the **Services** section:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 1.4: Get the registration token

Get the token provided in the `RegistrationToken.txt` file at `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` in the system where Citrix Infrastructure Monitor is installed and keep it ready for use in Step 2: Register Citrix Infrastructure Monitor.

PORT REQUIRMENTS

Once you successfully install `CitrixInfraMonitor.msi`, the installer creates an exception for the 9595 port. If you are using any third-party firewall, you might have to manually allow TCP communication for this port to use the Citrix Infrastructure Monitoring service.

The following table provides details on the inbound port requirements for Provisioning Service and StoreFront machines :

SOURCE	TARGET	TYPE	PORT	PROTOCOL	PURPOSE
Cloud Connector	Provisioning Service or StoreFront machine	TCP	9595	HTTP or HTTPS	Call to collect metrics from the Provisioning Service or StoreFront machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Provisioning Service and StoreFront machines don't make any outbound calls for the Infrastructure Monitoring service.

Step 2: Register Citrix Infrastructure Monitor

You can register Citrix Infrastructure Monitor using the following:

- Monitor UI
- Remote PowerShell SDK

Using Monitor UI

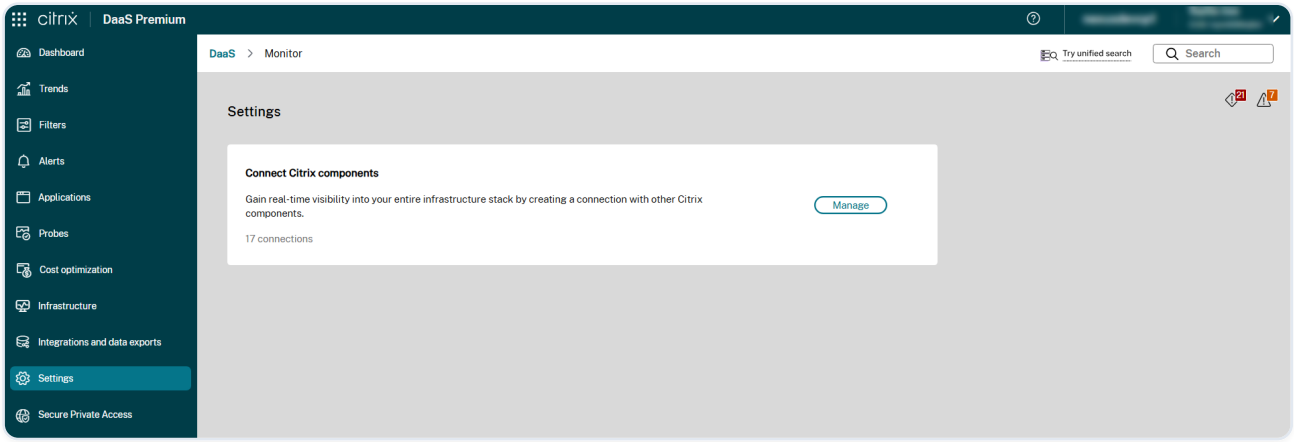
Complete the registration on the Monitor UI by performing the following steps.

STEP 2.1: NAVIGATE TO THE CONNECT CITRIX COMPONENTS PAGE

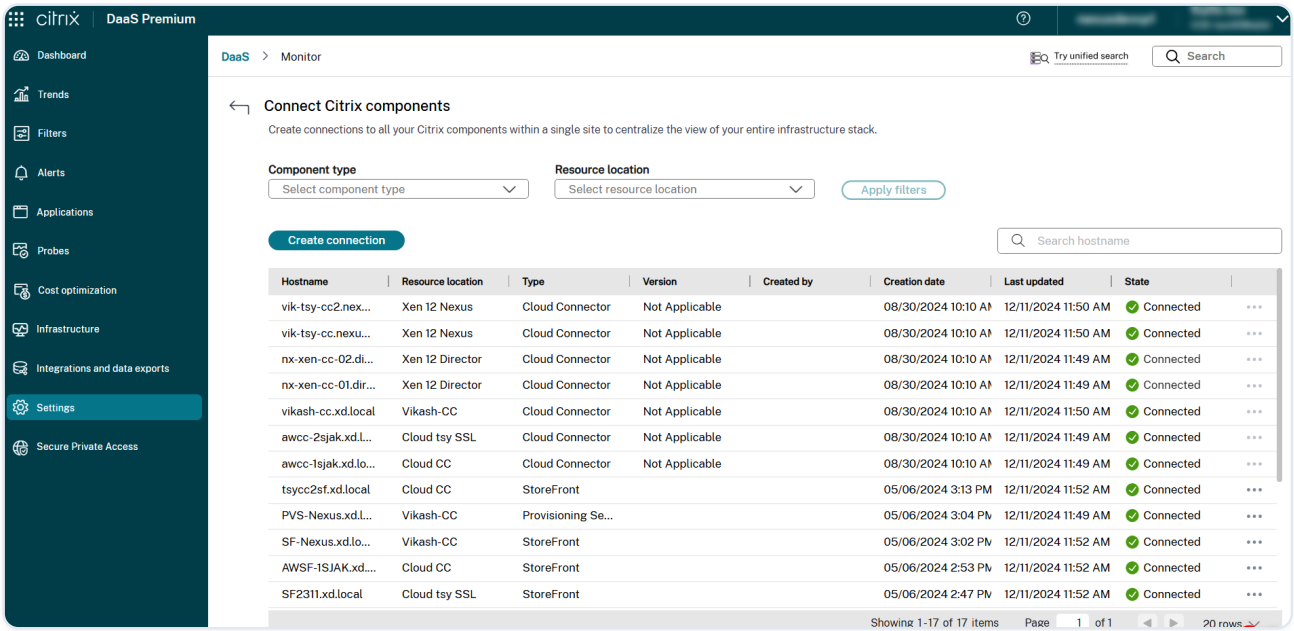
Click **Settings** > **Connect Citrix components** > **Manage**.

Or,

Click **Infrastructure** > **Manage**.

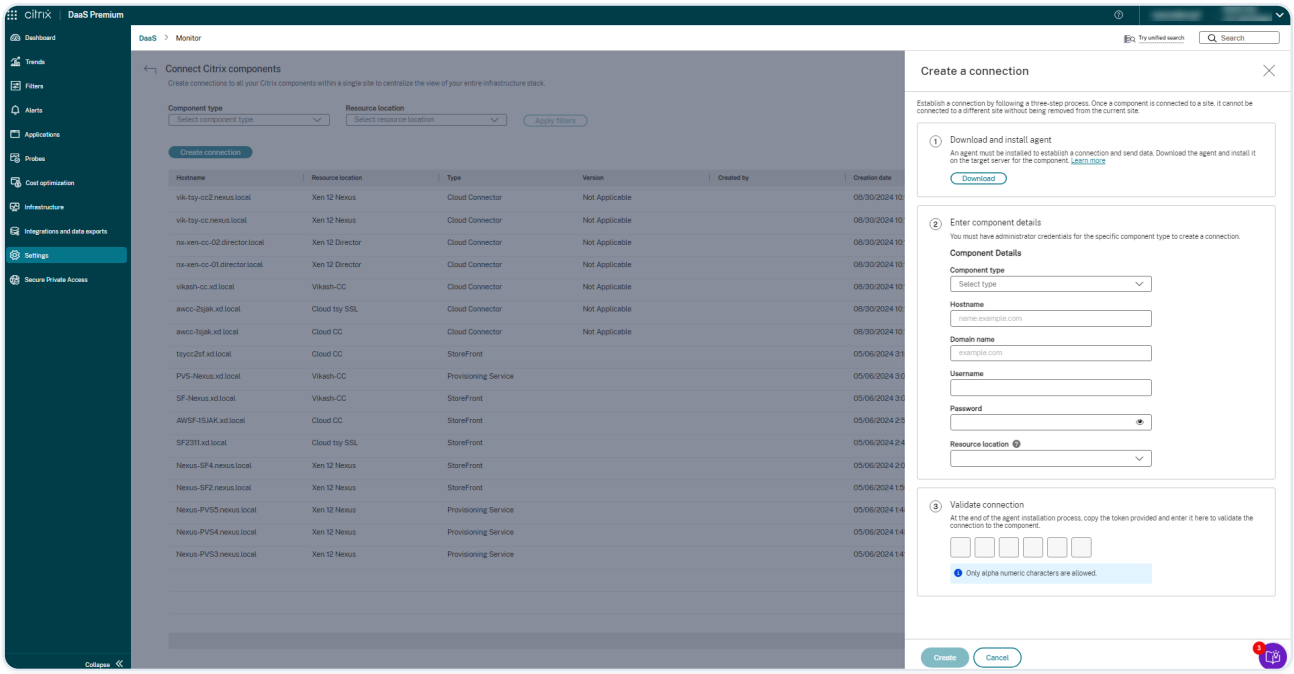


© 1997–2026 Citrix Systems, Inc. All rights reserved.



STEP 2.2: ENTER COMPONENT DETAILS

On the **Connect Citrix components** screen, click **Create connection**. The **Create a connection** window appears.



Ensure the `citrixinframonitor.msi` is downloaded and installed on the target. For more information, see Step 1 in this document. Follow the instructions on the screen, and populate the component details required to establish a secure connection.

- Select a **Component type** from the drop-down list. This can be Provisioning Service or StoreFront.
- Enter the **Hostname**.
- Enter the **Domain name**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Enter the **Username** of the Provisioning Service or StoreFront machine.
- Enter the **Password** of the Provisioning Service or StoreFront machine.
- Select the **Resource location**.

STEP 2.3: AUTHORIZE THE CONNECTION

Get the Citrix Infrastructure Monitor token from the `RegistrationToken.txt` file at `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` in the system where the Citrix Infrastructure Monitor is installed.

Enter the fetched token details in the Director UI. This authorizes the connection between the site and component.

The token text present in the `RegistrationToken.txt` file is regenerated when you restart the Citrix Infrastructure Monitor service. After the registration is successful, the token file is deleted from the machine. If you need to recreate a fresh token file for any reason, restart the Citrix Infrastructure Monitor service. For security reasons, the token file is removed after three failed registration attempts with an invalid token.

STEP 2.4: CREATE CONNECTION

Once the details are populated, click **Create**. The created connection is available under the list of connections on the **Connect Citrix components** page.

Using Remote PowerShell SDK

NOTE:

The minimum required version of PoshSDK is 7.42.26154.48609 or later.

1. Ensure the prerequistes mentioned at Prerequisites are met.
2. Set up Remote Powershell SDK.
3. Run the following PowerShell command to register the Citrix Infrastructure Monitor:

```
Add-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component> -AdminAddress localhost:19097 -ResourceLocationId
<resourceLocationID> -Domain <domain> -Username <username> -Password
<password> -Token <token>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The user name and password are optional parameters. However, if you don’t provide these parameters, some of the metrics won't be available for you.

The parameters of the preceding command are as follows:

PARAMETER	DESCRIPTION
`Fqdn`	FQDN of the Provisioning Service or StoreFront server.
`Component`	The component that you're onboarding. For example: Provisioning Service or SF. Provisioning Service stands for Citrix Provisioning™ and SF stands for StoreFront.
`ResourceLocationId`	The resource location ID of the site. To retrieve this value, select the **ID** button located beneath the resource location name on the **Resource Locations** page in Citrix Cloud.
`Domain`	The domain in which all components are a part of.
`Username`	User name of the admin user.
`Password`	Password of the admin user.
`Token`	Get the Citrix Infrastructure Monitor token from the `RegistrationToken.txt` file at `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` in the system where the Citrix Infrastructure Monitor is installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- The token text present at the `RegistrationToken.txt` file is regenerated when you restart the Citrix Infrastructure Monitor service. After the registration is successful, the token file is deleted from the machine. If you need to re-register, restart the Citrix Infrastructure Monitor service.
- For security reasons, the token file is removed after three failed registration attempts with an invalid token.

Once you successfully register the Provisioning Service or StoreFront machine, the machine name details appear on the **Monitor** > **Infrastructure** tab.

A sample command to register for the Citrix Infrastructure Monitor is as follows:

```
Add-MonitorDirectorAgent -Component PVS -Fqdn [redacted]
-ResourceLocationId [redacted] -Domain xd.local
-Username administrator -Password "[redacted]" -AdminAddress
localhost:19097 -Token [redacted]
```

Steps to Configure HTTPS for Citrix Infrastructure Monitor

NOTE:

Citrix Infrastructure Monitor service works in HTTP mode as well and in this case, the following configuration isn't required. However, we recommend you to use in https mode. **Perform the following steps only if you need to configure https for Citrix Infrastructure Monitor**.

Step 1: Upload the certificate to the machine

1. Get a PFX certificate for your machine where Citrix Infrastructure Monitor is installed. For more information on PFX file generation, see How to create a PFX file.

   NOTE:

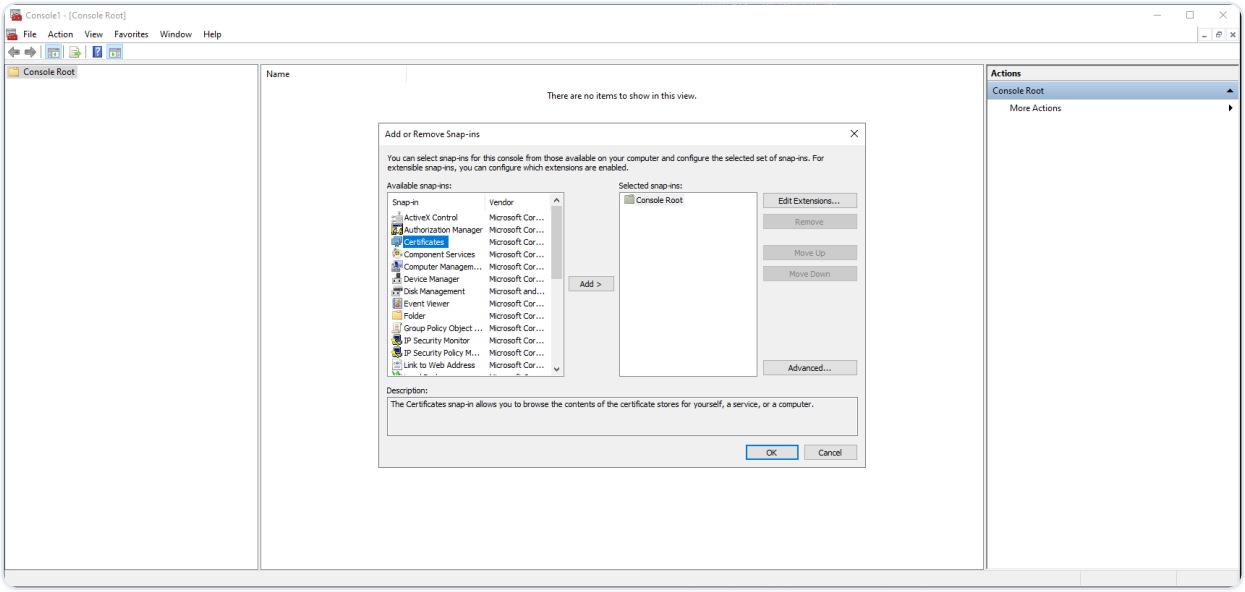
   You can use password protected PFX files also.

2. Upload the certificate to the machine to any location.

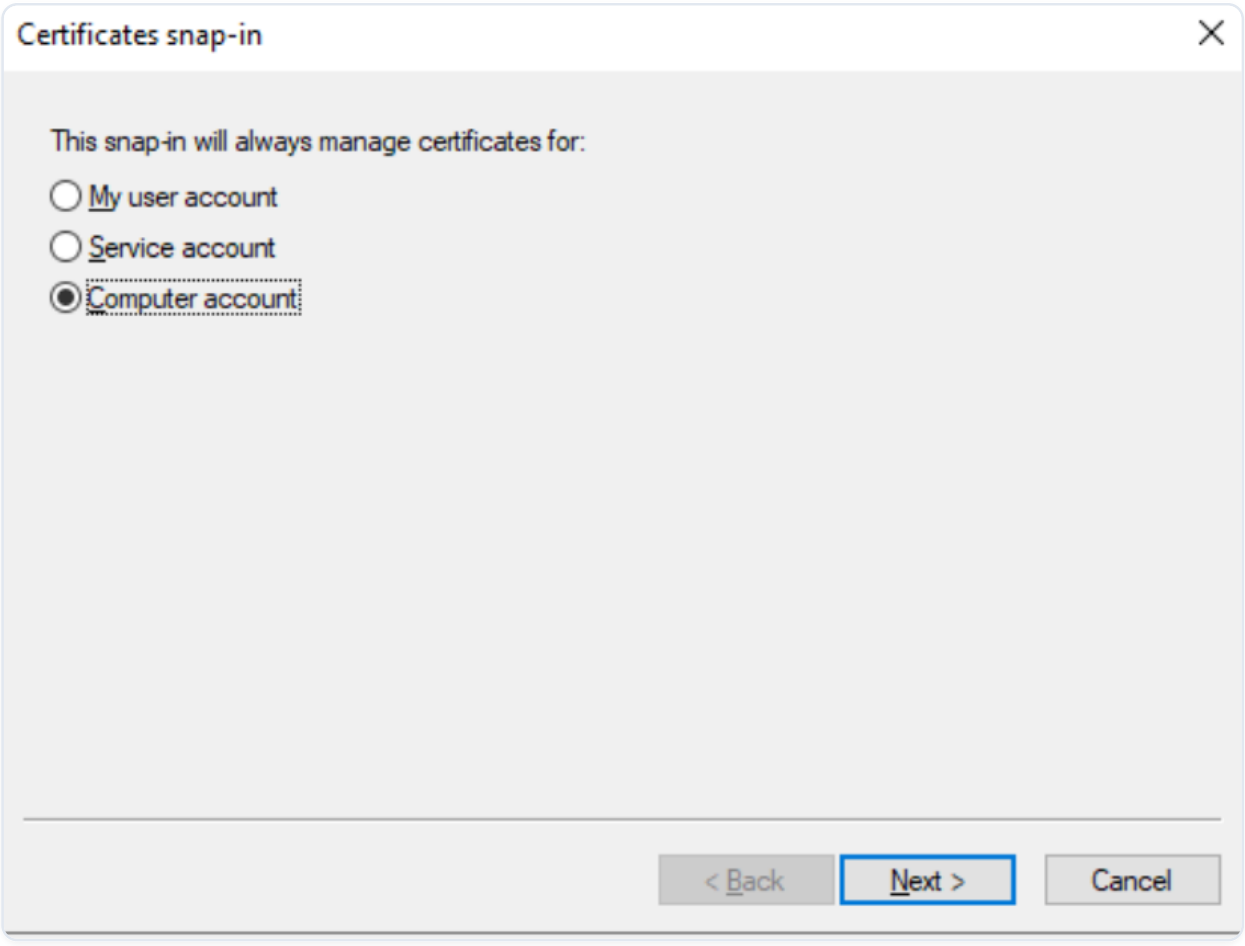
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Import the certificate to computer certificates

1. Click **Start** > **Run** > type `mmc`, and then click **OK**. The **Console 1 -** window appears.
2. On the **File** menu, click **Add/Remove Snap-in**. The **Add or Remove Snap-ins** window appears.

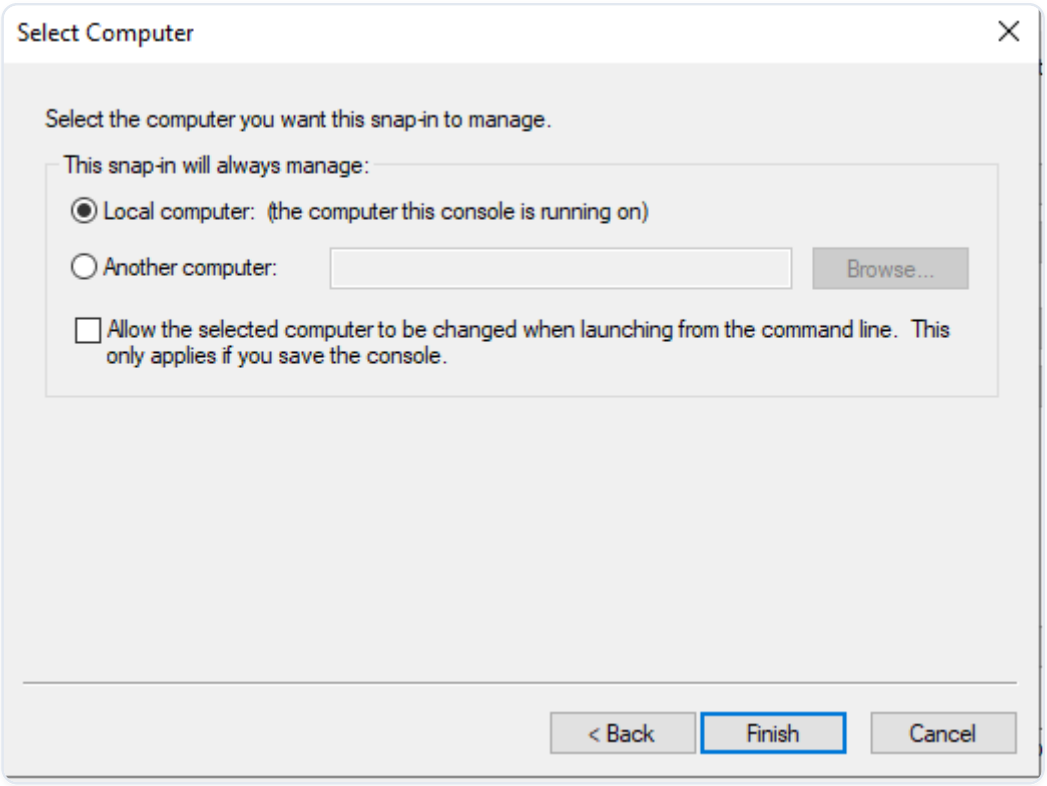


3. Under **Snap-in**, double-click **Certificates**. The **Certificates snap-in** window appears.

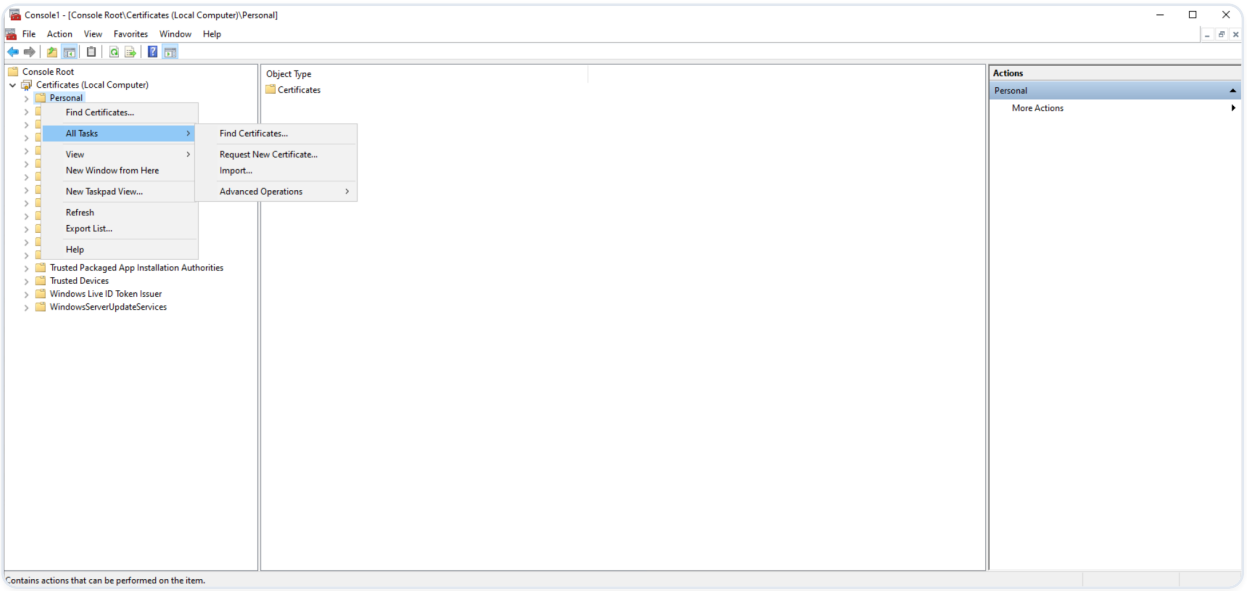


© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select **Computer account**, and then click **Next**. The **Select Computer** window appears.

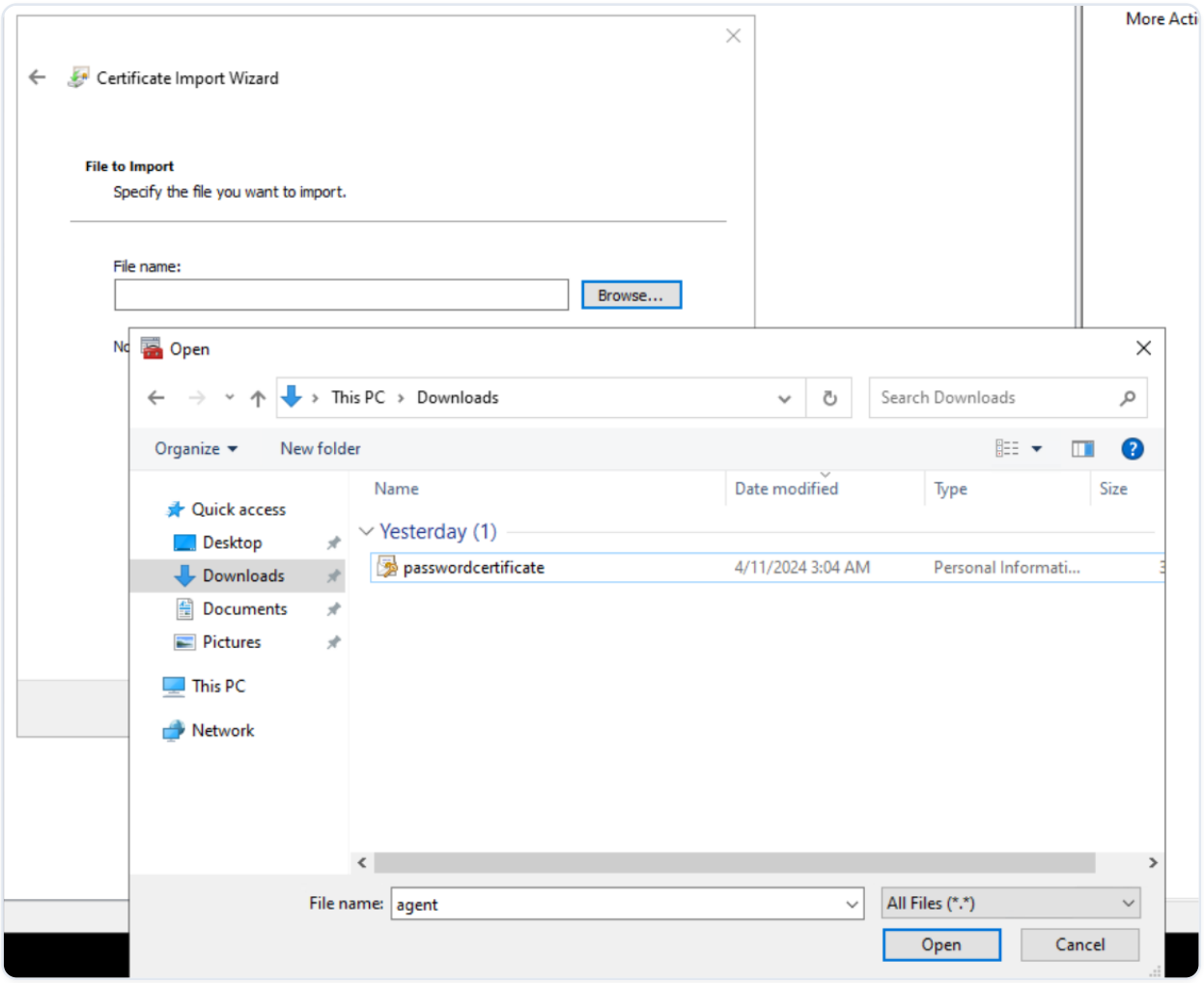


5. Select **Local computer**.
6. Click **Finish**. The **Certificates (Local Computer)** section appears on the list of selected snap-ins for the new console.
7. Click **OK**.
8. Expand **Certificates**, right-click **Personal** > **All Tasks** > **Import**. The **Welcome to the Certificate Import Wizard** appears.



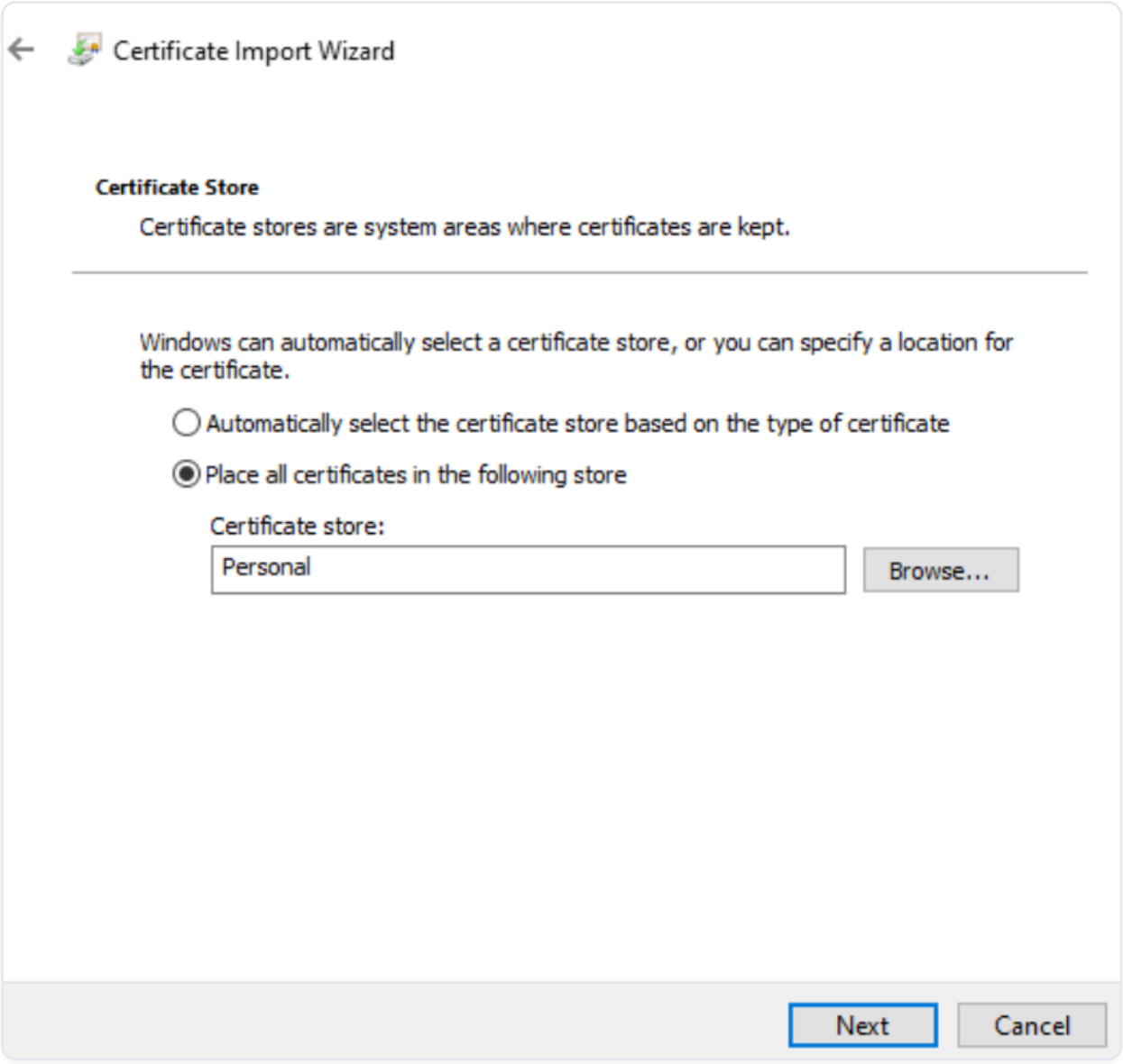
© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Select **Next** > **Browse Files**. Navigate to the location where you uploaded the PFX file, change the file type to **All files** and then select the respective PFX certificate.



10. Enter the PFX Password. You can leave it blank if there is no password.
11. Click **Next**.
12. For the Certificate Store, make sure that the **Place all certificates in the following store** option is selected and the **Certificate store** is selected as **Personal**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



13. Click **Next**.
14. Review the details and click **Finish**.
15. Wait for confirmation. The *The import was successful* message appears.
16. Navigate to **Certificates** > **Personal** and ensure that the certificate is present.
17. Delete the PFX certificate file from the machine.

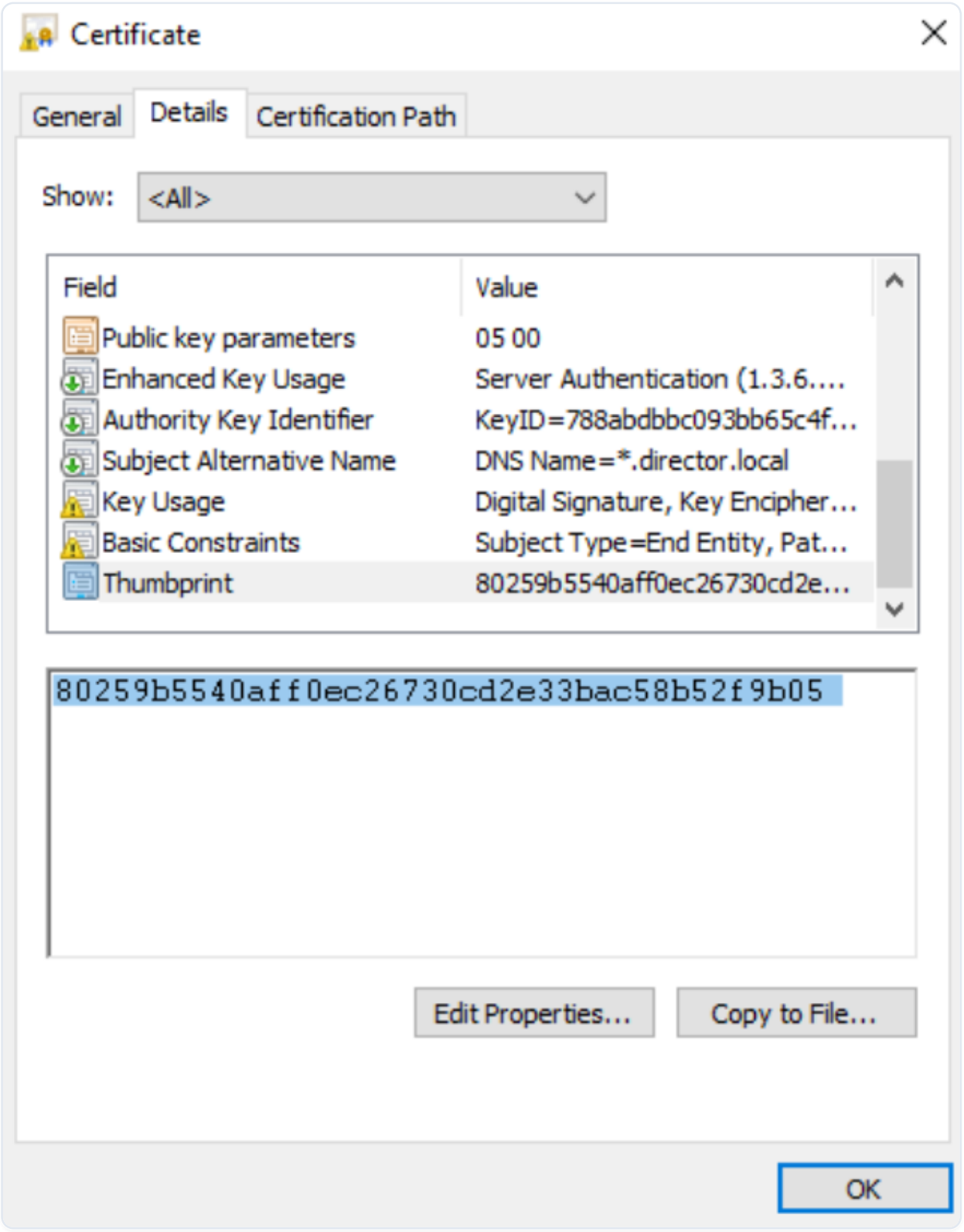
Step 3: Provide read access to certificate

1. Right-click on the imported certificate > **All Tasks** > **Manage Private Keys**.
2. In the dialog that opens, select **Add**, and then search for **Network Service**. Click **OK**.
3. Select **NETWORK SERVICE** under **Group** or **user names**.
4. Allow *Read* access under **Permissions for NETWORK SERVICE**.
5. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 4: Obtain the Thumbprint

1. Double-click on the imported certificate.
2. In the dialog that opens, navigate to the **Details** tab and scroll to the bottom.
3. Click **Thumbprint**.

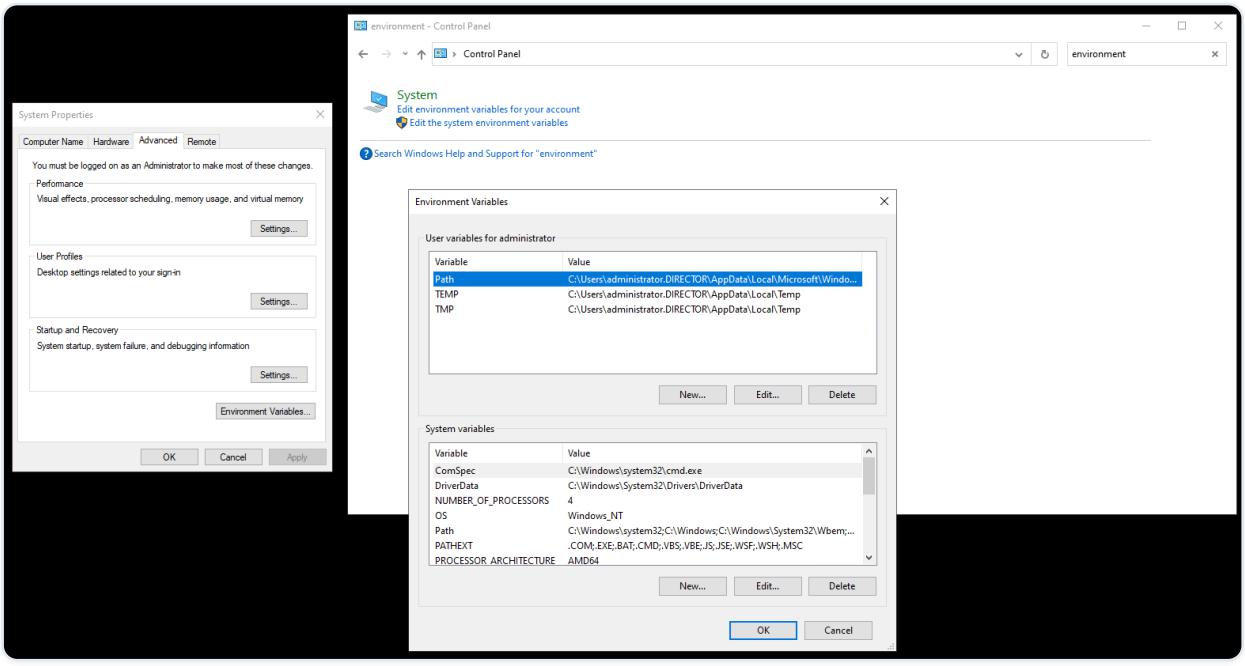


4. Copy the value and keep it ready for the next step.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 5: Setting the environment variable

1. Open Control Panel.
2. Search for environment and select **Edit the system environment variables**.
3. Under **System Variables (for all users)**, click **New**.



4. Specify the **Variable** name as *DIRECTOR_AGENT_HTTPS_CERTIFICATE_THUMBPRINT*.
5. Specify the thumbprint from the previous step under **Variable** value.
6. Click **OK**.

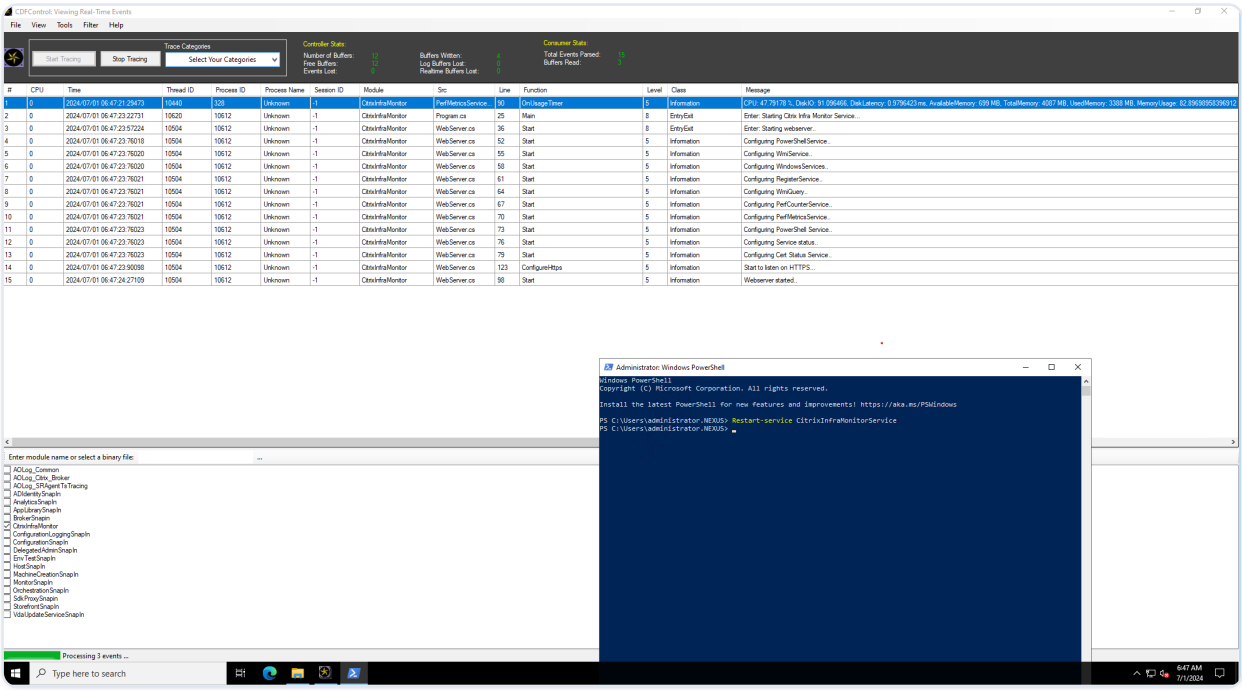
Step 6: Restart CitrixInfraMonitorService

1. Open PowerShell and run the following command:

```
Restart-Service CitrixInfraMonitorService
```

2. Ensure that the HTTPS is enabled by capturing the **CitrixInfraMonitorService** module and looking for the log line **Start to listen on HTTPS...**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 7: Enable HTTPs in Monitor configuration

You can enable HTTPs in Monitor service, using Remote PowerShell SDK.

NOTE:

The minimum required version of PoshSDK is 7.44.26401.2361 or later.

1. Ensure the prerequistes mentioned at Prerequisites are met.
2. Set up Remote Powershell SDK.
3. Run the following PowerShell command to enable HTTPS in Monitor configuration:

```
Set-DirectorAgentHttps -AdminAddress localhost:19097 -EnableHttps $true
```

NOTE:

To verify the existing settings value, run the `Get-DirectorAgentHttps -AdminAddress localhost:19097` command.

In case you need to disable HTTPS in Monitor configuration, run the `Set-DirectorAgentHttps -AdminAddress localhost:19097 -EnableHttps $false` command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set up Remote PowerShell SDK

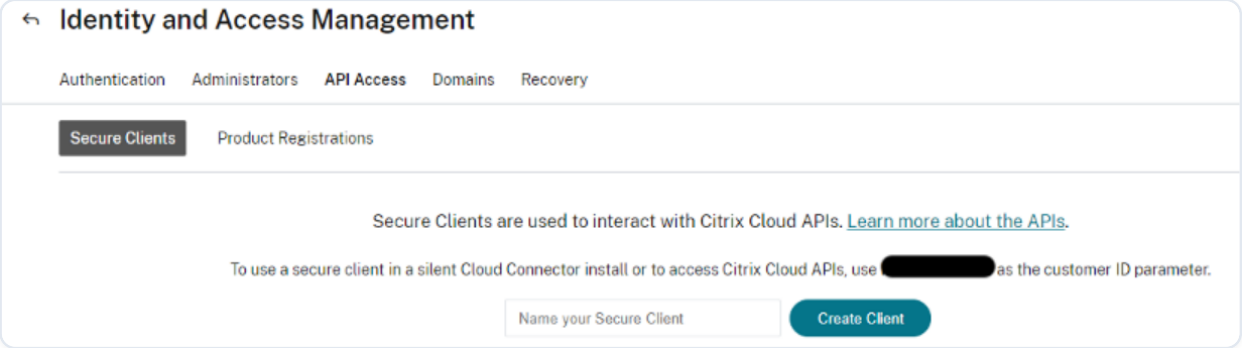
Prerequisites

- Ensure that the Citrix Infrastructure Monitor is installed on the StoreFront™ or Provisioning Service machine.
- You must first install the Remote PowerShell SDK on any domain-joined machine within the same resource location. For more information, see the SDK and API documentation.

Setting up of Remote PowerShell SDK

Perform the following steps and run the PowerShell commands on the device where you installed the Remote PowerShell SDK:

1. Sign in to the Citrix Cloud™ console with your Citrix Cloud credentials.
2. Navigate to **Identity and Access Management**.
3. Go to **API access** tab > **Secure Clients** > **Name your Secure Client** and click **Create Client**.



4. Once you've created the client, the ID and secret can be downloaded in a CSV file for future use.
5. To set up the connection with the Citrix Cloud environment, use the Client Secret created in the preceding step. The example command to use in PowerShell is as follows:

```
Set-XDCredentials -CustomerId “<customerid>” -SecureClientFile “c:
\temp\secureclient.csv” -ProfileType CloudAPI –StoreAs “default”
```

6. List the PowerShell Citrix Cloud profiles stored in the computer locally using the following PowerShell commands:

```
Get-XDCredentials -ListProfiles
```

   The following image shows the preceding commands as entered in the PowerShell:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

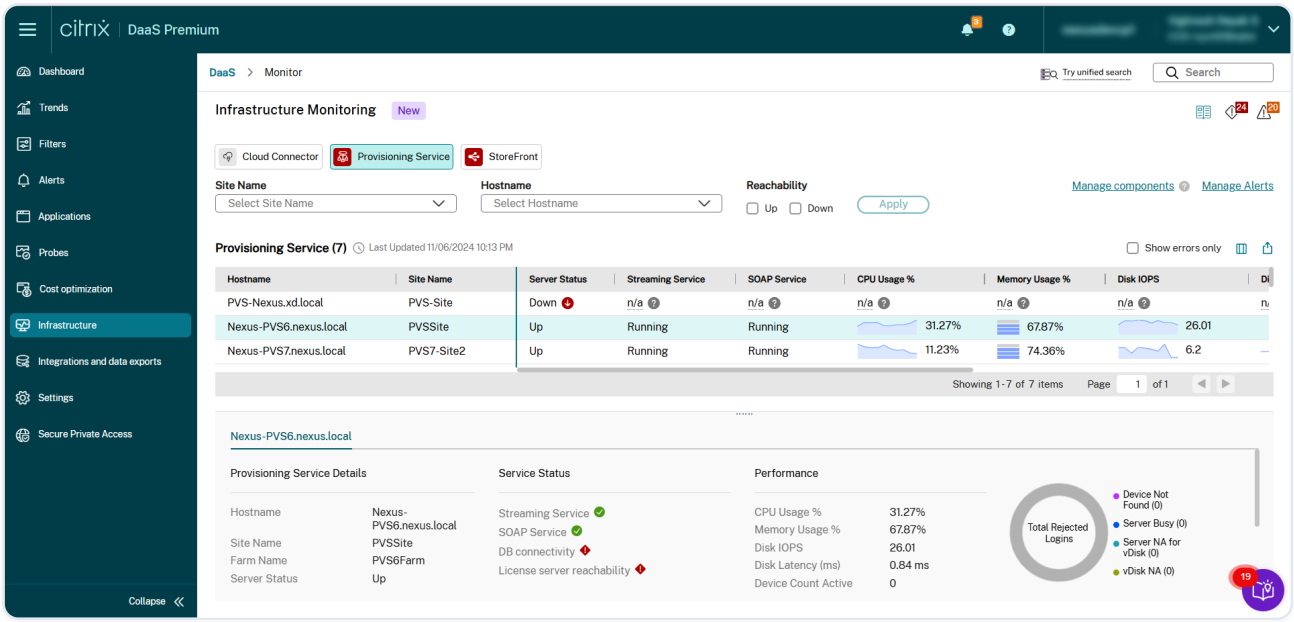
```
PS C:\WINDOWS\system32> Get-XDCredentials -ListProfiles

ProfileName ProfileType Credentials
----------- ----------- -----------
default         CloudApi Citrix.Sdk.Proxy.Cmdlets.Base.XDCredentials
```

For more information, see Citrix DaaS Remote PowerShell SDK.

Manage connections

You can view, remove, or edit the connections on the **Connect Citrix® components** page.



View connections

You can view details of all the connected and disconnected components available in this view. The following table describes the different columns of the **Create connection** page:

COLUMN	DESCRIPTION
Host name	The FQDN of the server.
Resource location	The resource location configured to reach the component.
Type	The type of the connection. This can be Provisioning Service and StoreFront.
Version	The version of the `CitrixInfraMonitor.msi` installed on the component.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COLUMN	DESCRIPTION
Created by	The name of the admin who created the connection.
Creation date	The date on which the connection is established.
Last updated	The date on which the connection was last updated.
State	The different states are Connecting, Connected, and Disconnected.
	• **Connecting**: This state indicates that it can take approximately five minutes for data to appear for the new component and approximately 10 minutes for the resource utilization data to be available.
	• **Connected**: This state indicates that the connection between the components and the site is up and running.
	• **Disconnected**: This state indicates that the connection between the components and the site is disconnected. Possible reasons for the Disconnected state include server downtime or the site being unable to connect to Citrix Infrastructure Monitor.

NOTE:

The Cloud Connector connections are automatically populated in this view when connected to the cloud site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Edit the connection

Editing the connection might be required to update the administrator credentials used to establish the Provisioning Service or StoreFront connection.

To edit an existing connection, do the following:

1. Navigate to the **Connect Citrix components** page from the **Settings** or **Infrastructure** tab.
2. On the list of connections table, click the three dots at the end of the row on the component of interest.
3. Click **Edit** and update the details as required.

Remove a component

You can do it from the Monitor UI or using the PowerShell command.

Using Monitor UI

Removing a component is a process of deregistering a Provisioning Service or StoreFront connection from Monitor. Once the deregistration process is complete, new data collection is stopped for the selected component. To remove an existing connection:

1. Navigate to the **Connect Citrix components** page from the **Settings** or **Infrastructure** tab.
2. On the list of connections table, click the three dots at the end of the row on the component of interest.
3. Click **Remove**. The connection is deregistered and removed from Monitor.

Using PowerShell command

In the event you need to deregister a given component, run the following PowerShell command on the device where PoshSDK is installed:

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component> -ResourceLocationId <resourceLocationID> -AdminAddress
localhost:19097
```

A sample command to remove registration of the Citrix Infrastructure Monitor is as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Remove-MonitorDirectorAgent -Component SF -Fqdn [redacted]
-ResourceLocationId [redacted] -AdminAddress
localhost:19097
```

NOTE:

Deregistering a component only stops the data flow from the specific component to Monitor. If you need to uninstall Citrix Infrastructure Monitor, uninstall it from the Control panel.

Infrastructure dashboard

You can see the health values for your components in the **Infrastructure Monitoring** page. These results help to analyze and troubleshoot issues proactively regarding your infrastructure.

You can filter the **Infrastructure Monitoring** page by:

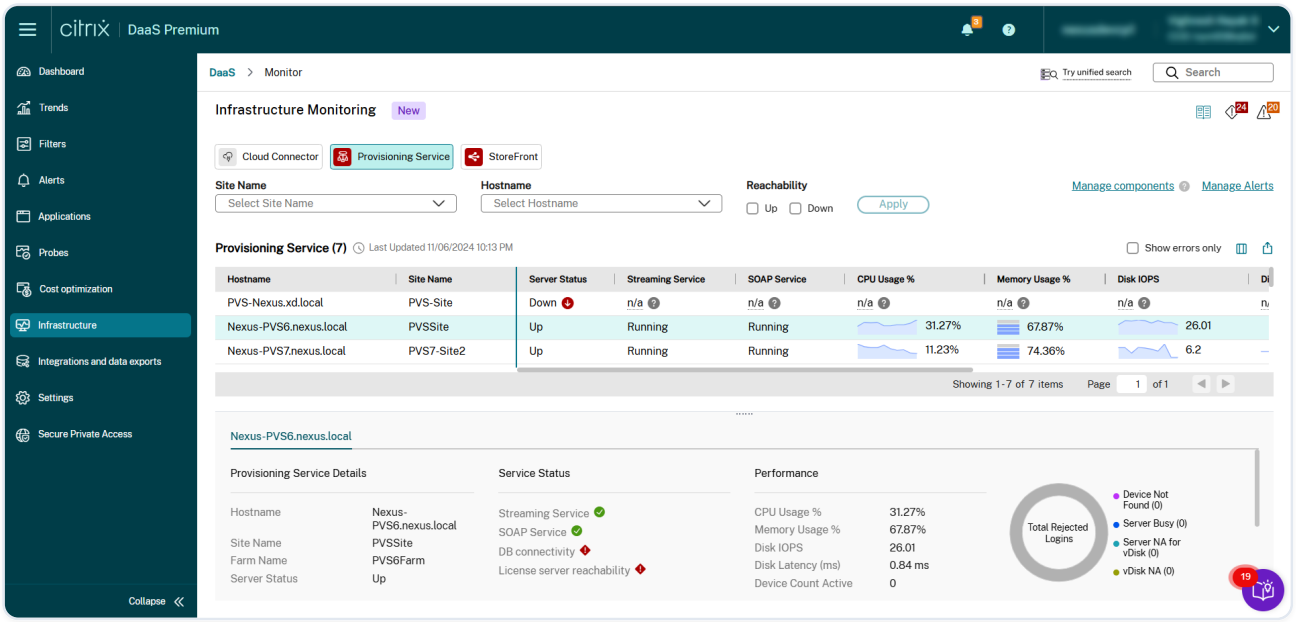
- Host name - Select the host name
- Reachability - Select **Up** (server is reachable) or **Down** (Server isn’t reachable) checkbox
- Errors - Select Show rows with errors only checkbox.

Use the **Manage columns** option to choose the data to be seen in your dashboard.

Provisioning Service health metrics

Click the **Infrastructure** tab and then select **Provisioning Service**. The Infrastructure dashboard for Provisioning Service appears:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following details are monitored for Provisioning Service servers:

CATEGORY	METRICS	DESCRIPTION
Reachability	Host name	The name of the Provisioning Service machine where Citrix Infrastructure Monitor is installed. This metric is a string value.
	Provisioning Service Site Name	The name of the Provisioning Service site. This metric is a string value.
	Provisioning Service Farm Name	The name of the Provisioning Service farm. This metric is a string value.
	Provisioning Service Site ID	Displays the site ID of the Provisioning Service server. This metric is a string value.
	Provisioning Service Farm ID	Displays the farm ID of the Provisioning Service server. This metric is a string value.
	Server Status	Shows the reachability state of the given server. Possible

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
		values are *Up*, *Down*, and *Unknown*.
	Last Boot Time	Displays the time when the Provisioning Service server was last booted.
	Last updated	Displays the time when the data was collected from the Provisioning Service server.
Dependent Services	Streaming Service	Displays the status of the streaming service. This metric shows the Windows services status. The possible values are: *Not running*, *Running*, *Not Installed*, and *n/a* (with help icon).
	SOAP Service	Displays the status of the Simple Object Access Protocol (SOAP) service. This metric shows the Windows services status. The possible values are: *Not running*, *Running*, *Not Installed*, and *n/a* (with help icon).
	DB Connectivity	Displays the status of the database connectivity. If you are using a Citrix Provisioning server version 2402 or earlier, you might get an unknown error. The possible values are *Not Connected*, *Connected*, *Unknown*, and *n/a* (with help icon).
	License Server Reachability	Displays whether the license server is reachable or not. If you're using the Citrix Provisioning server version

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
		2402 or earlier, you might get an unknown error. The possible values are *Not Connected*, *Connected*, *Unknown*, and *n/a* (with help icon).
Resource Utilization	CPU Usage %	Displays the usage of CPU in percentage using a line chart. The value displayed is the latest one at the end of the last 5 mins.
	Avg CPU %	Displays the average CPU percentage of the Provisioning Service server aggregated over the last 10 mins.
	Peak CPU %	Displays the peak CPU percentage of the Provisioning Service server in the last 5 mins.
	Memory Usage %	Displays the usage of memory in percentage using a stack chart. The value displayed is the latest one at the end of the last 5 mins.
	Avg Memory %	Displays the average memory percentage of the Provisioning Service server aggregated over the last 10 mins.
	Peak Memory %	Displays the peak memory percentage of the Provisioning Service server in the last 5 mins.

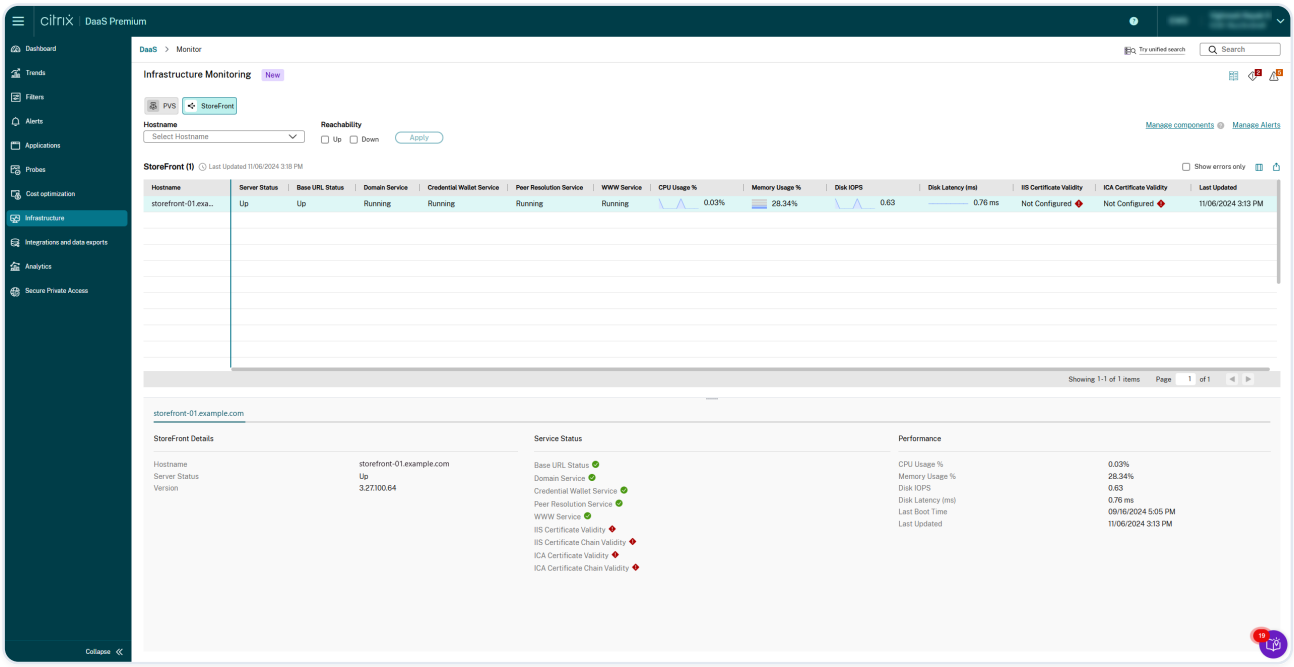
© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
	Disk IOPS	Displays the input and output value of the disk using a line chart.
	Avg Disk IOPS %	Displays the average disk IOPS of the Provisioning Service server aggregated over the last 10 mins.
	Peak Disk IOPS %	Displays the peak disk IOPS percentage of the Provisioning Service server in the last 10 mins.
	Disk Latency (Ms)	Displays the latency value of the disk using a line chart.
	Avg Disk Latency %	Displays the average disk latency of the Provisioning Service server aggregated over the last 10 mins.
	Peak Disk Latency %	Displays the peak disk latency percentage of the Provisioning Service server in the last 5 mins.
Impact	Total Rejected Logins	Number of total failure logins divided by the number of total logins trials.
	Device Count Active	Displays the total number of active devices in the Provisioning Service server. This metric is an integer value.

StoreFront™ health metrics

Click the **Infrastructure** tab and then select **StoreFront**. The Infrastructure dashboard for StoreFront appears:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following details are monitored for StoreFront servers:

CATEGORY	METRICS	DESCRIPTION
Reachability	Host name	Displays the name of the StoreFront server. This metric is a string value.
	Server Status	Displays the status of the StoreFront server. This metric shows the Windows services status. The possible values are: *Not running*, *Running*, *Not Installed*, and *n/a* (with help icon).
	Base URL Status	Displays the health of the base URL. If the HTTP status code is 200, the status is UP. Else, the value is Down.
	Last Boot Time	Displays the time when the StoreFront server was last booted.
	Last updated	Displays the time when the data was collected from the StoreFront server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
Dependent Services	Domain Service	Health of windows service named as domain service. This metric shows the Windows services status. The possible values are: *Not running*, *Running*, *Not Installed*, and *n/a* (with help icon).
	Credential Wallet Service	This service is a windows service that is used for storing encrypted passwords. The possible values are: *Not running*, *Running*, *Not Installed*, and *n/a* (with help icon).
	Peer Resolution Service	This service is a windows service which is responsible for inter-server group network communication forming a peer mesh of StoreFront servers. The possible values are: *Not running*, *Running*, *Not Installed*, and *n/a* (with help icon).
	WWW Service	This metric is the web service of the StoreFront server. This metric shows the Windows services status. The possible values are: *Not running*, *Running*, *Not Installed*, and *n/a* (with help icon).
Resource Utilization	CPU Usage %	Displays the usage of CPU in percentage using a line chart. The value displayed is the latest one at the end of the last five mins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
	Avg CPU %	Displays the average CPU percentage of the StoreFront server aggregated over the last 10 mins.
	Peak CPU %	Displays the peak CPU percentage of the StoreFront server in the last five mins. This value helps to decide on the maximum required capacity for a CPU.
	Memory Usage %	Displays the usage of memory in percentage using a stack chart. The value displayed is the latest one at the end of the last 5 mins.
	Avg Memory %	Displays the average memory percentage of the StoreFront server aggregated over the last 10 mins.
	Peak Memory %	Displays the peak memory percentage of the StoreFront server in the last 5 mins.
	Disk IOPS	Displays the input and output value of the disk using a line chart.
	Avg Disk IOPS %	Displays the average disk IOPS of the StoreFront server using a float.
	Peak Disk IOPS %	Displays the peak disk IOPS percentage of the StoreFront server aggregated over the last 10 mins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
	Disk Latency (Ms)	Displays the latency value of the disk using a line chart.
	Avg Disk Latency %	Displays the average disk latency of the StoreFront server aggregated over the last 10 mins.
	Peak Disk Latency %	Displays the peak disk latency percentage of the StoreFront server in the last five mins.
Impact	ICA® Certificate Validity	Displays the validity of the ICA certificate. The possible values are *Expired*, *Expiring*, *Valid*, and *Not Found*.
	ICA Certificate Chain Validity	Displays StoreFront ICA Certificate Chain is valid or not. The possible value is *Yes* or *No*.
	IIS Certificate Validity	Displays the validity of the IIS certificate. The possible values are *Expired*, *Expiring*, *Valid*, and *Not Found*.
	IIS Certificate Chain Validity	Displays StoreFront IIS Certificate Chain is valid or not. The possible value is *Yes* or *No*.

Cloud Connector health metrics

The Cloud Connector component is added by default as part of Infrastructure monitoring. The Cloud Connector component that is connected to the Citrix DaaS™ site is auto onboarded for monitoring.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature enables customers to monitor Cloud Connector's health under the infrastructure monitoring dashboard and configure alerts for it. The alerting functionality enables customer admins to get alerted if any of the policies created for Cloud Connectors are in the critical or warning stage.

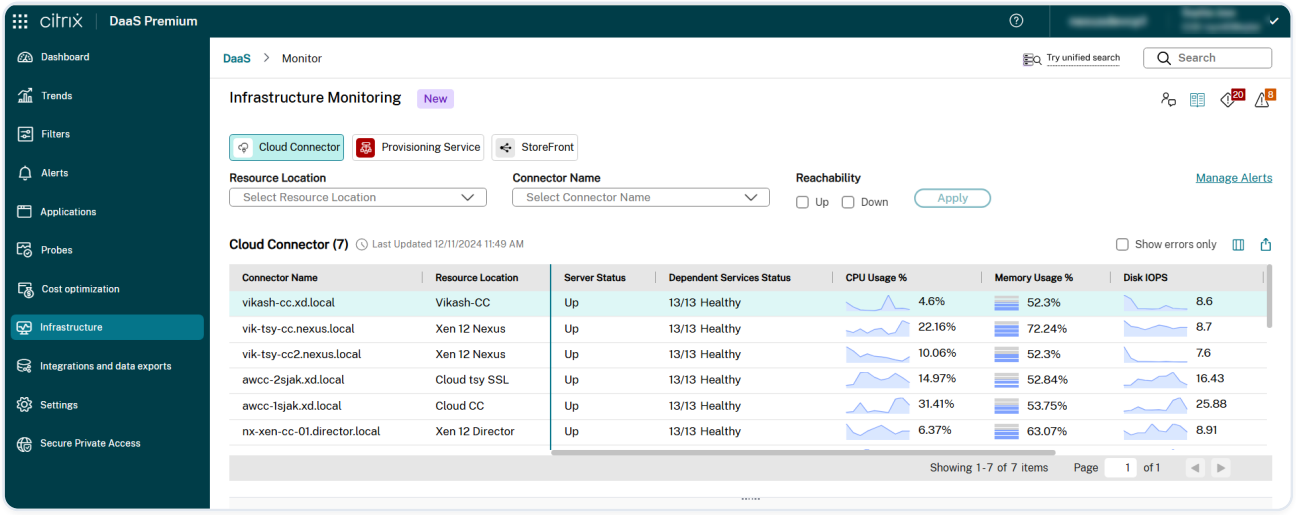
You can select the required **Component** type and the details are displayed according to the selected site name. You can also select the **Resource location**.

NOTE:

The `citrixinframonitor.msi` file is not required for monitoring Cloud Connectors.

You can monitor both single-site and multi-site details for the infrastructure details.

Click the **Infrastructure** tab and then select **Cloud Connector**. The infrastructure dashboard for Cloud Connector appears:



The following details are monitored for Cloud Connector:

CATEGORY	METRICS	DESCRIPTION
Reachability	Server Status	Shows the reachability state of the given Cloud Connector. Possible values are *Up* and *Down*.
	Dependent Service Status	Provides the summary of the Cloud Connector Dependent Service status. The possible values are **13/13 Running** (when all services are

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
		running) or `<number of stopped services>/13 Not Running` (shows services which are not running on the tooltip).
	Version	The version of the Cloud Connector.
	Last Boot Time	Displays the time when the Cloud Connector was last booted.
	Last updated	Displays the latest time when the data was collected from the Cloud Connector.
Dependent Services-This metric shows the Windows services status. The possible values are: Unknown, Not running, Start Pending, Stop Pending, Running, Continue Pending, Pause Pending, Paused, and Not Installed.	Citrix Connection Lease Exchange service	Displays the status of the Citrix Connection Lease Exchange service which enables Connection Lease files to be exchanged between the Citrix Workspace™ app and Cloud Connector for Service Continuity for Workspace.
	Citrix AD Provider	Displays the status of the Citrix AD Provider service which enables Citrix Cloud™ to facilitate management of resources associated with the Active Directory domain accounts in which it is installed.
	Citrix Agent Discovery	Displays the status of the Citrix Agent Discovery service which enables Citrix Cloud to facilitate management of XenApp and XenDesktop®

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
		legacy on-premises Citrix products.
	Citrix Credential Provider	Displays the status of the Citrix Credential Provider which handles storage and retrieval of encrypted data.
	Citrix NetScaler® Cloud Gateway	Displays the status of the Citrix NetScaler Cloud Gateway which provides Internet connectivity to on-premises desktops and applications without the need to open in-bound firewall rules or deploying components in the DMZ.
	Citrix Agent Logger	Displays the status of the Citrix Agent Logger which provides a support logging framework for the Citrix Cloud Connector™ services.
	Citrix WebRelay Provider	Displays the status of the Citrix WebRelay Provider which enables HTTP Requests received from WebRelay Cloud service to be forwarded to on-premises Web Servers.
	Citrix High Availability Service	Displays the status of the Citrix High Availability service which provides continuity of service during outage of a central site.
	Citrix Remote HCL Server	Displays the status of the Citrix Remote HCL Server which proxies communications between the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
		Delivery Controller™ and the Hypervisors.
	Citrix Remote Broker Provider	Displays the status of the Citrix Remote Broker Provider which enables communication to a remote Broker Service from local VDAs and StoreFront servers.
	Citrix CDF Capture Service	Displays the status of the Citrix CDF Capture service which captures CDF traces from all configured products and components.
	Citrix Config Synchronizer	Displays the status of the Citrix Config Synchronizer which copies brokering configuration locally for high availability mode.
	Citrix Agent WatchDog	Displays the status of the Citrix Agent WatchDog which monitors and upgrades the on-premises agents (evergreen).
Resource Utilization	CPU Usage %	Displays the usage of CPU in percentage using a line chart. The value displayed is the latest one at the end of the last 5 mins.
	Average CPU %	Displays the average CPU percentage of the Cloud Connector server aggregated over the last 10 mins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
	Peak CPU %	Displays the peak CPU percentage of the Cloud Connector server in the last 5 mins.
	Memory Usage %	Displays the usage of memory in percentage using a stack chart. The value displayed is the latest one at the end of the last 5 mins.
	Average Memory %	Displays the average memory percentage of the Cloud Connector server aggregated over the last 10 mins.
	Peak Memory %	Displays the peak memory percentage of the Cloud Connector server in the last 5 mins.
	Disk IOPS	Displays the input and output value of the disk using a line chart.
	Average Disk IOPS %	Displays the average disk IOPS of the Cloud Connector server aggregated over the last 10 mins.
	Peak Disk IOPS %	Displays the peak disk IOPS percentage of the Cloud Connector server in the last 10 mins.
	Disk Latency (Ms)	Displays the latency value of the disk using a line chart.
	Average Disk Latency %	Displays the average disk latency of the Cloud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
		Connector server aggregated over the last 10 mins.
	Peak Disk Latency %	Displays the peak disk latency percentage of the Cloud Connector server in the last 5 mins.

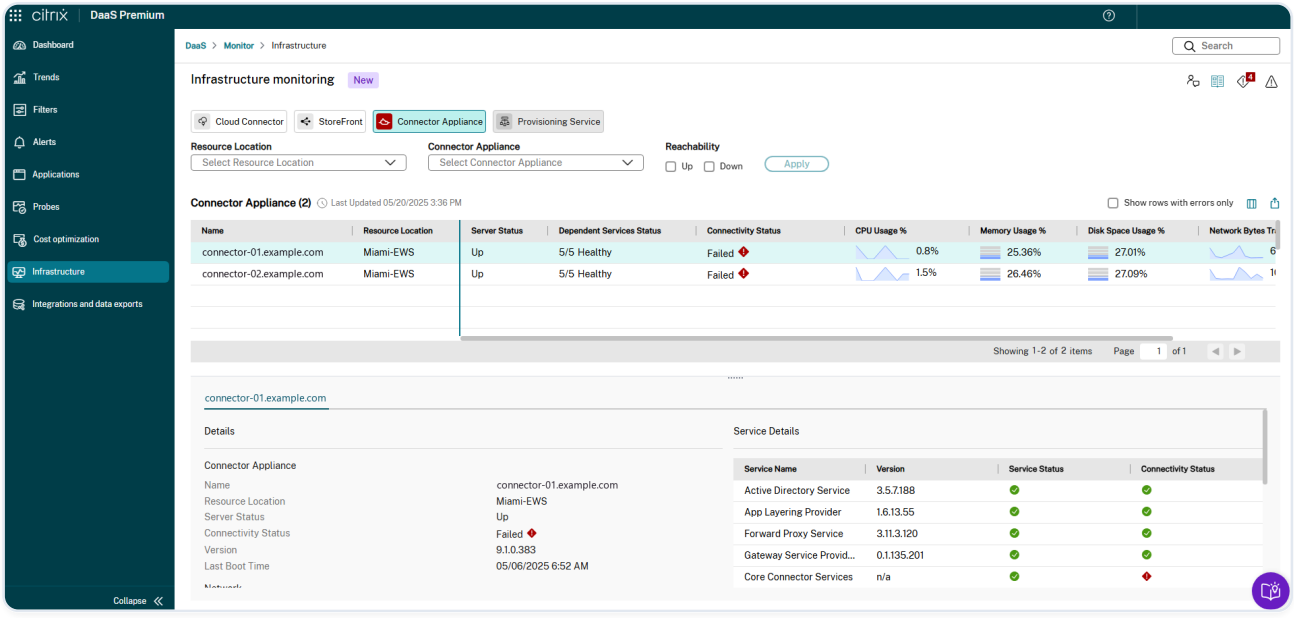
Connector Appliance health metrics

The **Connector Appliance** component is added by default as part of Infrastructure monitoring. The **Connector Appliance** component that is connected to the Citrix DaaS site is auto onboarded for monitoring.

This feature enables customers to monitor Connector Appliance's health under the Infrastructure monitoring dashboard.

You can select the required **Component** type and the details are displayed according to the selected site name. You can also select the **Resource location**.

Click the **Infrastructure** tab and then select **Connector Appliance**. The infrastructure dashboard for Connector Appliance appears:



The following details are monitored for Connector Appliance:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
Reachability	Server Status	Shows the reachability state of the given Connector Appliance. Possible values are *Up* and *Down*. Connector Appliance sends status events to Citrix every 5 minutes, the *Down* state occurs when no events have been received for 20 consecutive minutes.
	Dependent Service Status	Provides the summary of the Connector Appliance Dependent Service status. Possible values are **5/5 Running** (when all services are running) or `<stopped>/5 Not Running`.
	Connectivity Status	Displays whether the service can reach the addresses in Citrix Cloud necessary for it to operate. Possible values are *Success* and *Failed*.
	Version	The version of the Connector Appliance.
	Last Boot Time	Displays the time when the Connector Appliance was last booted.
	Last updated	Displays the latest time when the data was collected from the Connector Appliance.
	Proxy Details	Displays the proxy that the Connector Appliance uses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
Network	Public IP v4	Displays the public IP address of the Connector Appliance.
	Private IP	Displays the private IP address of the Connector Appliance.
Authentication	AD Configured	*True* or *False* to indicate if the Connector Appliance Server has configured AD.
	Joined domains	Displays the domain that the Connector Appliance has joined.
Dependent Services	Active Directory Service	Enables integration with the Active Directory, allowing authentication and management of users across multiple domains.
	App Layering Provider	Connects the Citrix App Layering™ appliance to Active Directory, enabling directory junctions for managing user attributes.
	Gateway Service	Facilitates secure access to Citrix Cloud services, ensuring seamless connectivity between on-premises resources and cloud environments.
	Forward Proxy Service	Helps manage outbound connections, ensuring secure and efficient communication between Citrix Cloud and enterprise networks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
	Core Connector Services	Enables communication between Citrix Cloud and resource locations, supporting authentication, image portability, and other cloud management functions.
Resource Utilization	CPU Usage %	Displays the usage of CPU in percentage using a line chart. The value displayed is the latest one at the end of the last 5 mins.
	Average CPU %	Displays the average CPU percentage of the Connector Appliance server aggregated over the last 10 mins.
	Peak CPU %	Displays the peak CPU percentage of the Connector Appliance server in the last 10 mins.
	Memory Usage %	Displays the usage of memory in percentage using a stack chart. The value displayed is the latest one at the end of the last 5 mins.
	Average Memory %	Displays the average memory percentage of the Connector Appliance server aggregated over the last 10 mins.
	Peak Memory %	Displays the peak memory percentage of the Connector Appliance server in the last 10 mins.
	Disk Space Usage %	Displays the usage of disk space in percentage using a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	METRICS	DESCRIPTION
		stack chart. The value displayed is the latest one at the end of the last 5 mins.
	Average Disk Space Usage %	Displays the average disk space usage percentage of the Connector Appliance server aggregated over the last 10 mins.
	Peak Disk Space Usage %	Displays the peak disk space usage percentage of the Connector Appliance server in the last 10 mins.
	Network Bytes Transferred Per Minute	Displays the network bytes transferred per minute using a line chart. The value displayed is the latest one at the end of the last 5 mins.
	Average Network Bytes Transferred Per Minute	Displays the average network bytes transferred per minute of the Connector Appliance server over the last 10 mins.
	Peak Network Bytes Transferred Per Minute	Displays the peak network bytes transferred per minute of the Connector Appliance server over the last 10 mins.

Create and manage alerts

You can set up alerts for proactively monitoring conditions and scopes of interest to you and reduce alert fatigue. Alerts can be configured with severity, re-alert intervals, notification mediums, and follow the alert lifecycle supported in the product.

For more information, see the following:

- Alerts
- Advanced alert policies

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application and Desktop Probing

Application and desktop probing automates the process of checking the health of the apps and desktops that are published in a site by test launching them serially using StoreFront. The results of probing are available in the **Monitor** console of Citrix DaaS. Citrix Probe Agent supports all sites including those hosted on Citrix Cloud™ Japan and Citrix Cloud Government Control Planes.

Requirements

- Endpoint machines running probe agents are Windows machines with Citrix Workspace™ app for Windows version 1808 or later for application probing and version 1906 or later for desktop probing. Workspace app for Unified Windows Platform (UWP) is not supported.
- Citrix Probe Agent supports the default form-based authentication as supported by Citrix® StoreFront Cloud. In cases where the endpoint device is connected to a store using Citrix Gateway, you can authenticate using the Citrix Gateway domain credentials or Multi-factor authentication (MFA). Citrix Probe Agent doesn't support other authentication methods like Single Sign-On (SSO). Similarly, Citrix Probe Agent works only when there is no proxy server or load balancer like Citrix Gateway or Citrix ADC deployed.
- Application and Desktop probing is available in Citrix DaaS™ Premium and Citrix DaaS Premium Plus.

  NOTE:

  - If user enabled the sign-in policy or conditional authentication on Citrix Cloud, probe agent fails to sign in to Storefront™ or Citrix Workspace app.
  - Probe Agent supports only the Active Directory authentication to authenticate to Citrix Workspace app.

- Ensure that Microsoft .NET Framework version 4.7.2 or later is installed on the endpoint machine where you want to install the Probe Agent.
- To use the probing agent in Citrix Cloud Japan Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" to 2. To use the probing agent in Citrix Cloud Government Control Plane, set the registry value in the path, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" to 3.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User accounts/permissions required to run Probing:

- A unique user to probe on each endpoint machine. The user is not required to be an administrator; the probes can run in a non-admin context.
- User accounts with Windows administrator permissions to install and configure the Citrix Probe Agent on the endpoint machines.
- User must be a member of the same domain as the VDAs used for application or desktop launch. Probe Agent currently doesn't support multiple domains.
- Reusing existing user accounts for probing might log off from the users' active sessions. A full administrator user account or a custom role with the following permissions:
    - Delivery group permissions:
        - Read-only
    - Director permissions:
        - Create\\Edit\\Remove Alert Email Server Configuration - if the email server is not already configured
        - Create\\Edit\\Remove Probe Configurations
        - View Configurations page
        - View Trends page

Configuration

You can schedule your probes to run during off-peak hours across multiple geographies. The comprehensive probe results can help to troubleshoot issues related to the applications, hosting machine or connection before the users experience them.

Citrix Probe Agent version 2103 supports site aggregation. Applications and desktops can be enumerated and launched from aggregated sites. When you configure the probe agent, select the **Workspace (StoreFront) Site Aggregation Enabled** option to enable enumeration of applications and desktops from aggregated sites. The following combinations of sites are supported:

- Multiple on-premises sites having one store URL.
- On-premises and cloud sites having either an on-premises store URL or a cloud store URL.
- Multiple cloud sites having one store URL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

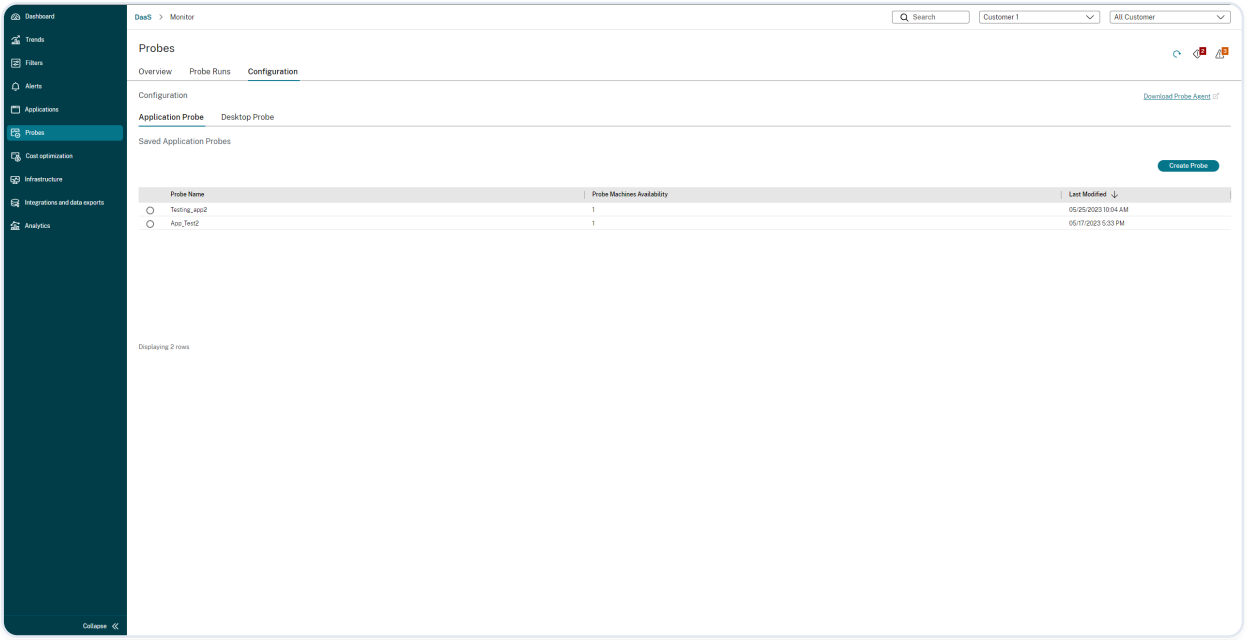
NOTE:

You must create separate administrators or users to configure probes that have access to only one site.

Step 1: Install and configure the Citrix Probe Agent

The Citrix Probe Agent is a Windows executable that simulates the actual application or desktop launch by the user through StoreFront. It tests launches as configured in Monitor and reports back the results to Monitor.

1. Identify endpoint machines from where you want to run probing.
2. Users with administrative privileges can install and configure the Citrix Probe Agent on the endpoint machine. Download the Citrix Probe Agent executable available in the Citrix downloads page.



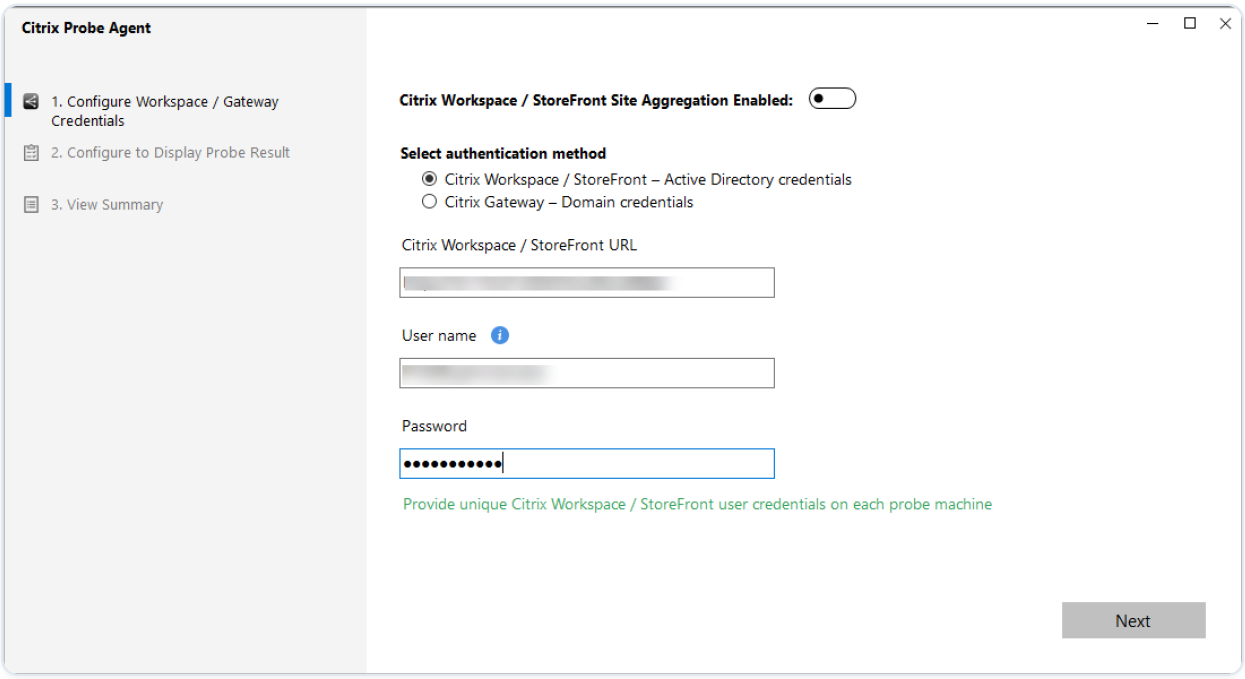
3. Start the agent and enter the credentials of an appropriate user. Configure a unique user on each endpoint machine. The credentials are encrypted and stored securely.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES:

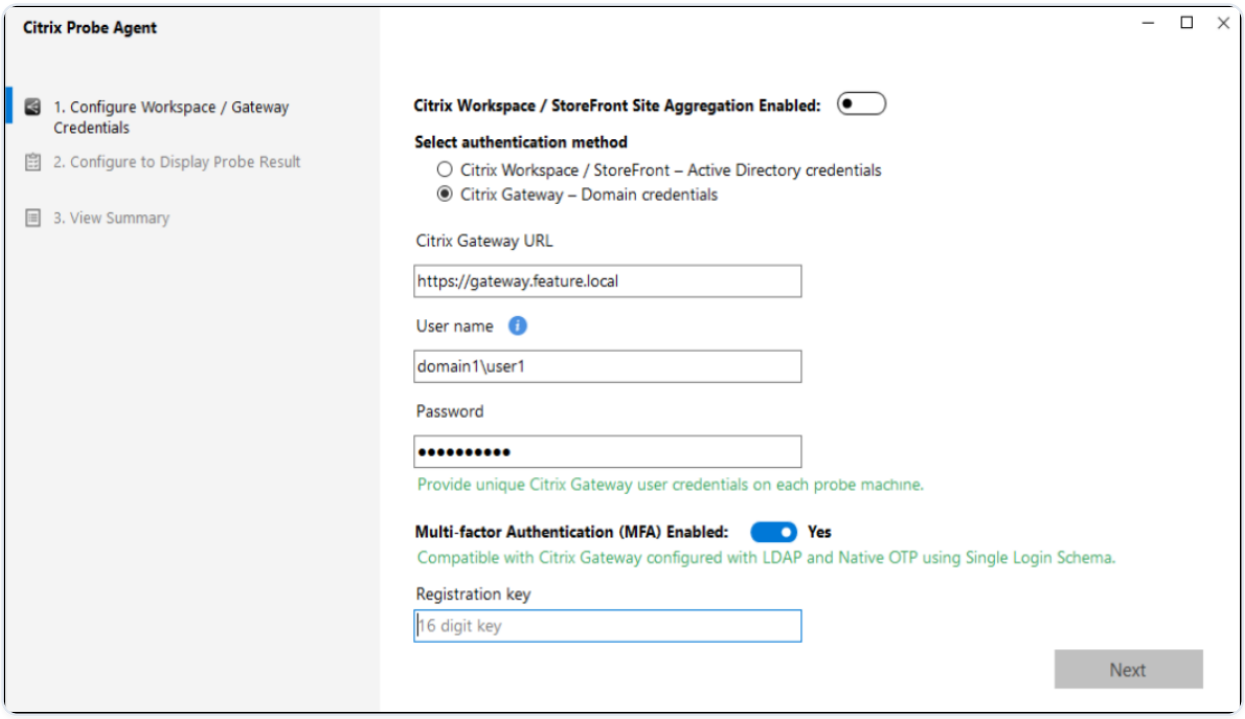
- To access the site to be probed from outside the network, type the login URL for Citrix Gateway in the **store URL** field. Citrix Gateway automatically routes the request to the corresponding site store URL.
- Use NetBIOS as the domain name in the user name field. For example, NetBIOS/username.
- App probing supports Citrix Content Collaboration™ service using authentication (AD only).

4. Select an authentication method and enter the relevant credentials. Credentials are encrypted and stored securely.
5. Configure with your StoreFront Active Directory credentials. Configure a unique user on each endpoint machine.

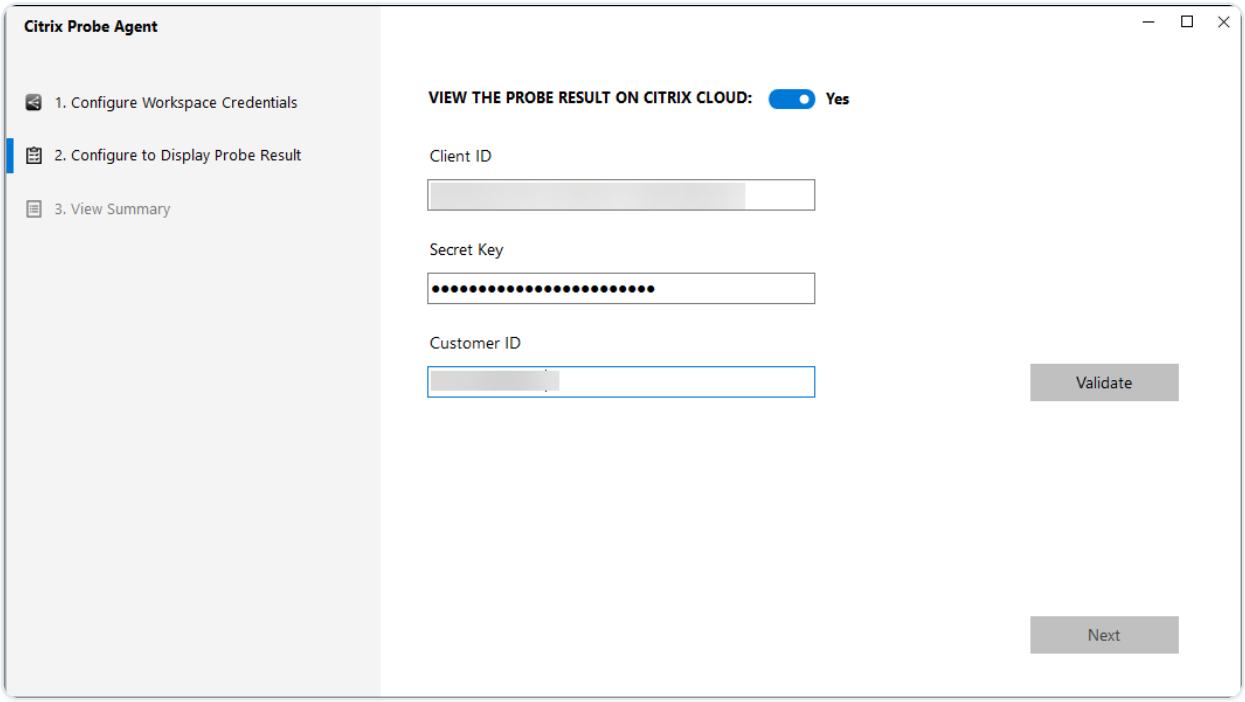


6. Choose the Citrix Gateway option if your endpoint is connected to StoreFront via Citrix Gateway and configure with your Citrix Gateway Domain credentials.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. Choose Multi-factor Authentication option if your Gateway supports it and enter the 16-digit authentication key. This is available only for Citrix Gateway that is configured with LDAP and Native OTP using Single Login Schema.
8. In the **Configure To Display Probe Result** tab, enter credentials to access Citrix DaaS. You can find the Customer Name or Customer ID, Client ID, and Secret Key from the API Access page in the Citrix Cloud console.



9. Select your site and click Next.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. In the **View Summary** tab, ensure that the configured details are accurate. If you need to make changes, go to the respective tab and make the updates.

Step 2: Configure Probing in Monitor

LIMITATION:

Probing fails if applications or desktops are test launched from Windows VDAs that have the interactive logon message banner enabled. This is because a timeout occurs due to waiting to accept the interactive logon message. To disable the logon message on a Server VDA. Go to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security options.

Remove the text in the following fields and update the Microsoft policy.

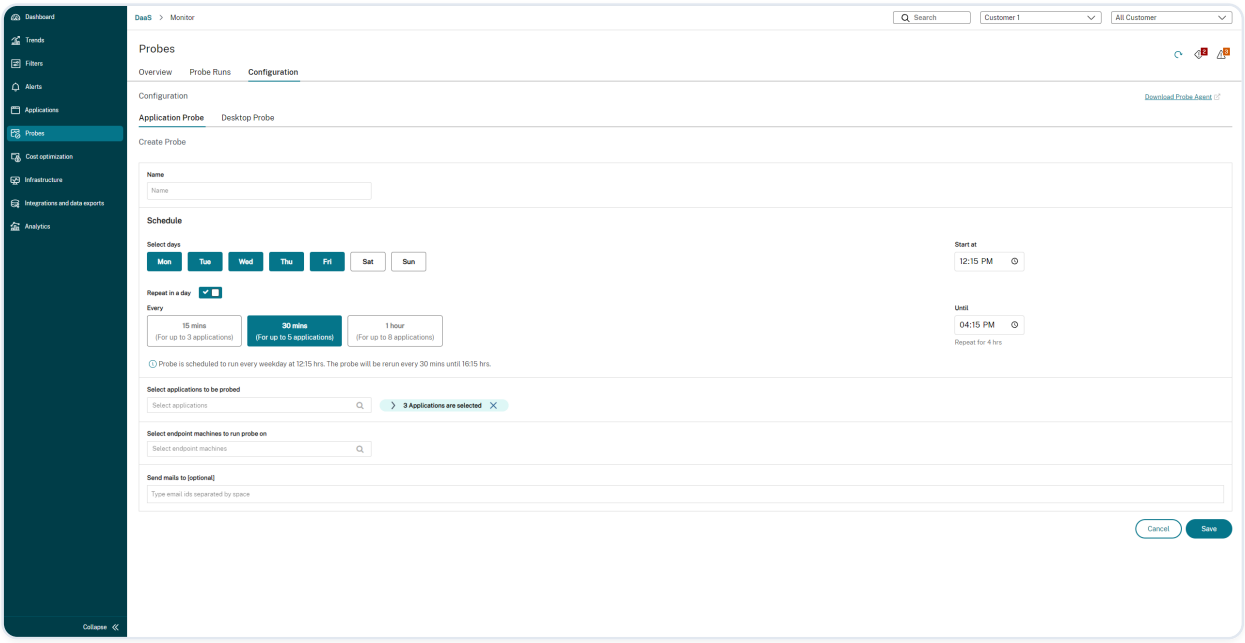
- Interactive Logon: Message Text for users attempting to logon
- Interactive Logon: Message Title for users attempting to logon

Assign the probe user to this specific Server VDA with the interactive logon message banner disabled to ensure that the probe can get past the Application or Desktop Launch State.
For more information, see `<https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`.

1. Go to **Configuration** \> **Probe Configuration** \> **Application Probe** or **Desktop Probe** and click **Create Probe**.
2. In the **Create Probe** page, enter the name of the probe.
3. Select the schedule:
    a. Choose the days of the week on which you want the probe to run.
    b. Enter the start time at which you want the probe to run.
    c. In addition, you can choose the **Repeat in a day** option. Enter the end time and the interval in which you want the probe to repeat within a day. For example, the configuration below helps run application probes from 12:08 hours until 16:34 hours repeating every 30 minutes every Monday, Wednesday, Thursday, and Sunday.
4. Select the recommended number of applications or desktops to be probed depending on the interval.
5. Select the endpoint machines on which the probe must run.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Enter the email addresses to which the failure probe results are sent. Configure your email server in **Alerts** > **Email Server Configuration**.



In this configuration, the application sessions launch at 12:08 hours, 12:38 hours, 13:08 hours, and so on until 16:08 hours every Monday, Wednesday, Thursday, and Sunday.

NOTE:

- After configuration, the agent runs the configured probes starting the next hour.
- The probes that were set up before the **Repeat in a day** option was introduced, continue to run at their scheduled time. They have the **Repeat in a day** option disabled by default.
- It is recommended that you configure probes such that each run has a period of 5 minutes to prevent overlaps.

Step 3: Probe execution

The agent runs probing as per the probe configuration that it fetches from Monitor periodically. It launches selected applications or desktops serially using Workspace. The agent reports the results back to Monitor via the Monitor database. Failures are reported in five specific stages:

- **Workspace Reachability** - configured store URL is not reachable.
- **Workspace Authentication** - configured StoreFront credentials are invalid.
- **Workspace Enumeration** - Workspace Enumerate applications list does not contain the application or desktop to be probed.

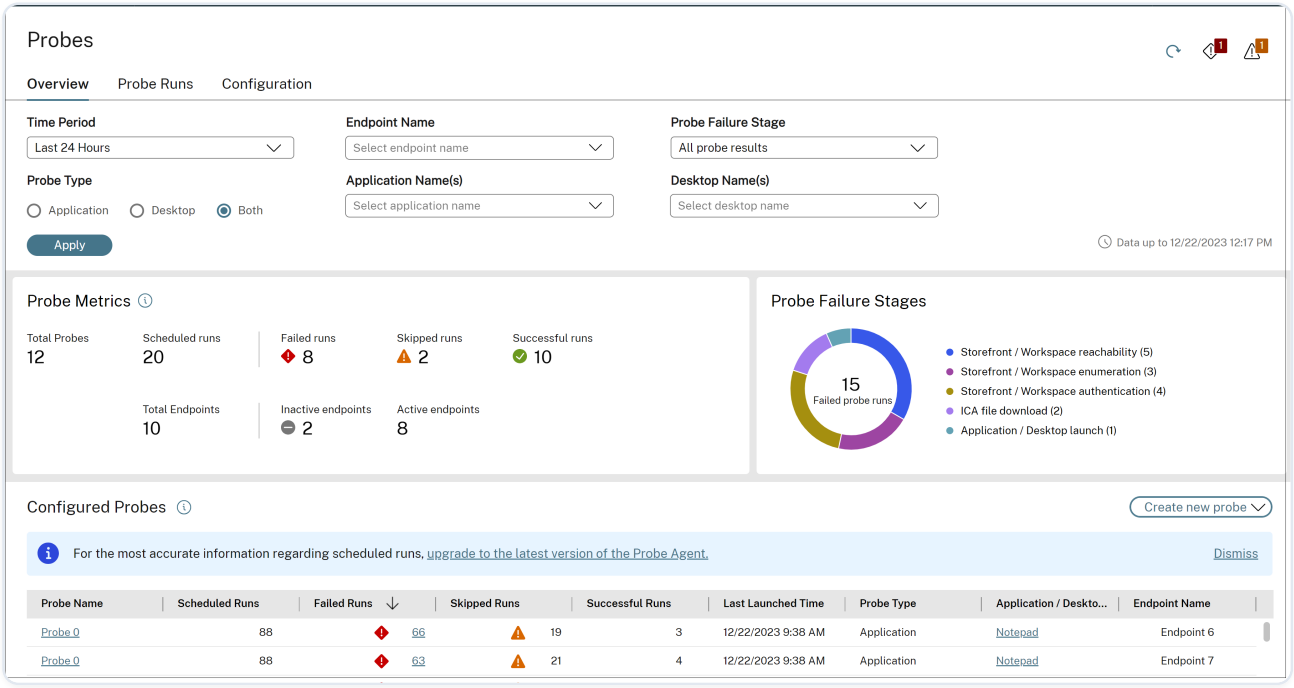
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ICA® download** - the ICA file is not available.
- **Application / Desktop launch** – the application or desktop could not be launched.

Step 4: View probe results

You can see the probe results in **Probes**. The Probes view gives a comprehensive glimpse of the probe results. These results help analyze and troubleshoot issues proactively, enabling a smoother session launch experience for users.

The **Overview** tab provides a summary of all the configured probes in a single view.



You can filter probes based on Time Period, Probe Type, Endpoint name, Application Name, Desktop Name and Probe Result Type. Probes that match the filter criteria are shown with the following details per probe, application/desktop and endpoint.

Probe Metrics shows the count of Scheduled, Planned, Skipped, Successful, and Failed runs.

- Completed Runs – the number of probe runs that ran to completion.
- Failed Runs – the number of probe runs that failed.
- Skipped Runs – The number of skipped runs is equal to the number of scheduled runs minus the sum of failed runs and successful runs.
- Successful Runs – the number of probes that completed successfully with no failures in any stage during the app/desktop launch.

The total number of endpoint machines is also displayed, with the count of active and inactive machines.

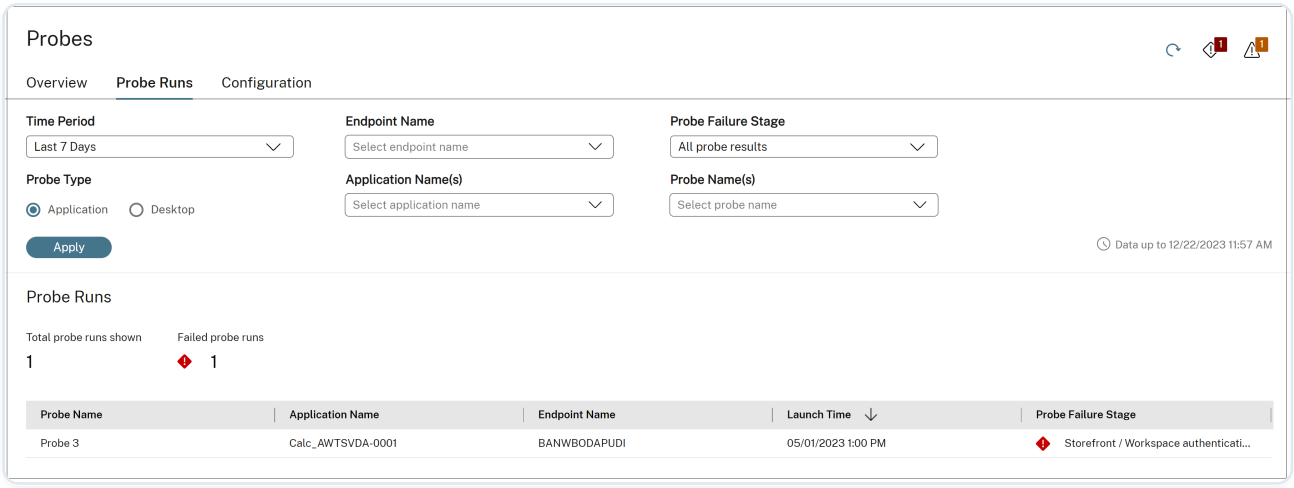
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Probe Failure Stages presents a visual breakdown of the failure distribution for each failure group. By analyzing the stages in which most failures have occurred, it becomes easier to interpret the probe results and troubleshoot issues. The graphical representation shows the number of failed probe runs for application/desktop launch, ICA file downloads, Storefront/Workspace enumeration, Storefront/Workspace reachability, and Storefront/Workspace authentication.

It helps analyze the stages in which most failures have occurred. This information helps quickly understand the probe results and troubleshoot.

Some probe runs might not run to completion due to either the endpoint being inactive, or services being unavailable.

The **Probe Runs** tab provides the results of the completed probe runs in detail. You can drilldown to see the details of each individual run of a selected probe. You can filter and analyze further based on important pivot points.



You can filter the probes runs based on Time Period, Probe Type, Endpoint name, Application Name, Desktop Name and Probe Failure Stage. Probe Failure Stage displays the stage in which the probe failed. Clicking on the Probe Name, Scheduled Runs, Failed Runs, Application/ Desktop name links also takes you to the Probe Runs page with the list of Probe runs matching the filter criteria.

Cost optimization

Citrix Monitor now introduces a new feature called Cost Optimization, which helps you to analyze the usage of virtual machines and sessions effectively. This feature provides insightful visual representations on how to optimize the cost. It also helps you to eliminate unnecessary machines and thereby reducing costs.

To support the cost optimization, the following alerts are also introduced:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Failed power on action and Failed Power off action
- Machine uptime alert

You can also inspect machines with recent power actions to analyze power-on failure which causes user issues and power off failure which increase costs. For more information, see the Inspect machines with recent power actions section.

Click the **Cost Optimization** tab from the left menu on the **Home** page to access the **Cost Optimization** page.



On the **Cost Optimization** home page, you can do the following:

- Get started link - Access this link to learn more about the cost optimization feature.
- Review the cost optimization page - You can provide feedback on the **Cost Optimization** page
- Refresh the data.
- View the alerts - You can view both critical and warning alerts.
- Export data

The **Cost Optimization** page includes the following features:

- Cost savings
- Workload rightsizing

How is the cost calculated for cost optimization

The cost per machine per hour is displayed in the currency that the hypervisor supports. This section describes how cost is calculated for Azure machines and for other machines.

Cost for Azure machines

The order of priority for calculating the cost is as follows:

1. When the 'Microsoft.Consumption/pricesheets/read permission is available, the effective price is displayed in the currency that is configured in the Azure subscription. This method to calculate cost is in preview.
2. If permissions aren’t available, the Azure retail price is displayed. For more information, see Azure Retail Prices overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

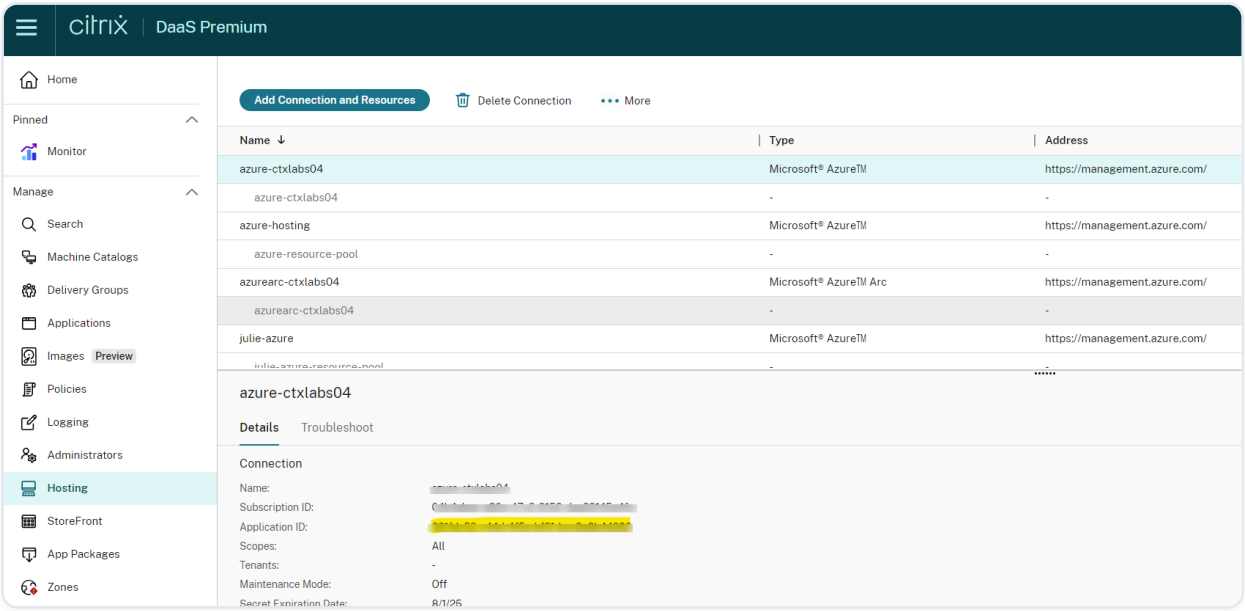
NOTE:

Make sure you have access to the `https://prices.azure.com` endpoint to enable retrieval of either the effective price or the retail price details.

3. When the effective price or retail price isn't available, the cost is displayed based on the cost entered by admins in the Web Studio. For more information, see Machine cost section of the documentation.
4. If there's no cost mentioned in the Web Studio, the default cost of $1 is considered.

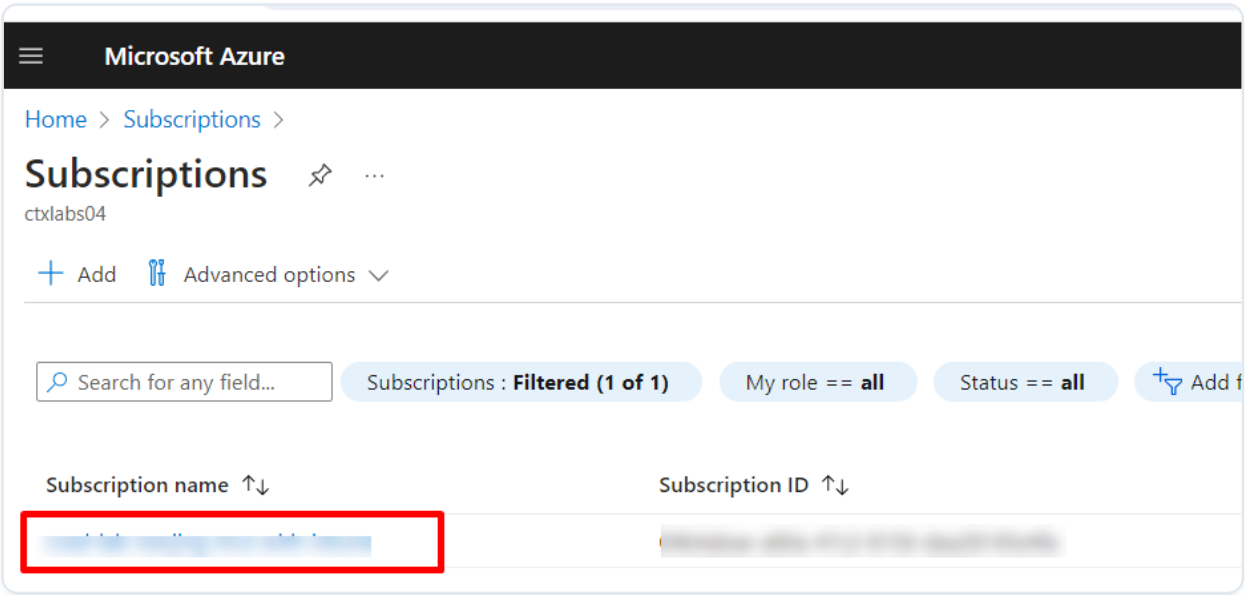
To find the account details of Azure and add the required permission to find the effective price, do the following:

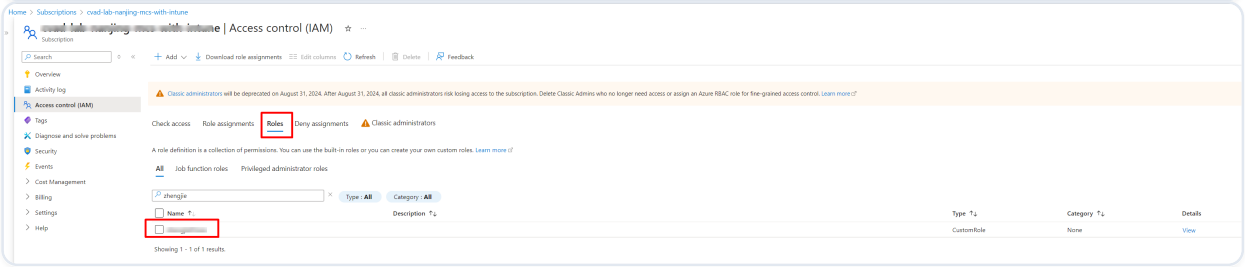
1. Navigate to Citrix DaaS.
2. Click the **Hosting** tab to find the hosting connection account.
3. Look for the **Application ID** mentioned in the **Hosting** tab.



4. Go to the Microsoft Entra ID and look for the **Application ID** noted in step 3.
5. Go to **Subscription** > **Access control (IAM)** > choose a customized role configured for the hosting connection SPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





6. Add the *Microsoft.Consumption/pricesheets/read* permission to the role.

How to verify the Azure retail price

If the `Microsoft.Consumption/pricesheets/read` isn't available, the Azure retail price is displayed. Now you can use the Retail Rates Prices API to get retail prices for all Azure services. Previously, the only way that you can retrieve prices for Azure services was to either use the Azure Pricing Calculator or use the Azure portal. For more information, see Azure Retail Prices overview.

Calculating costs for machines other than Azure

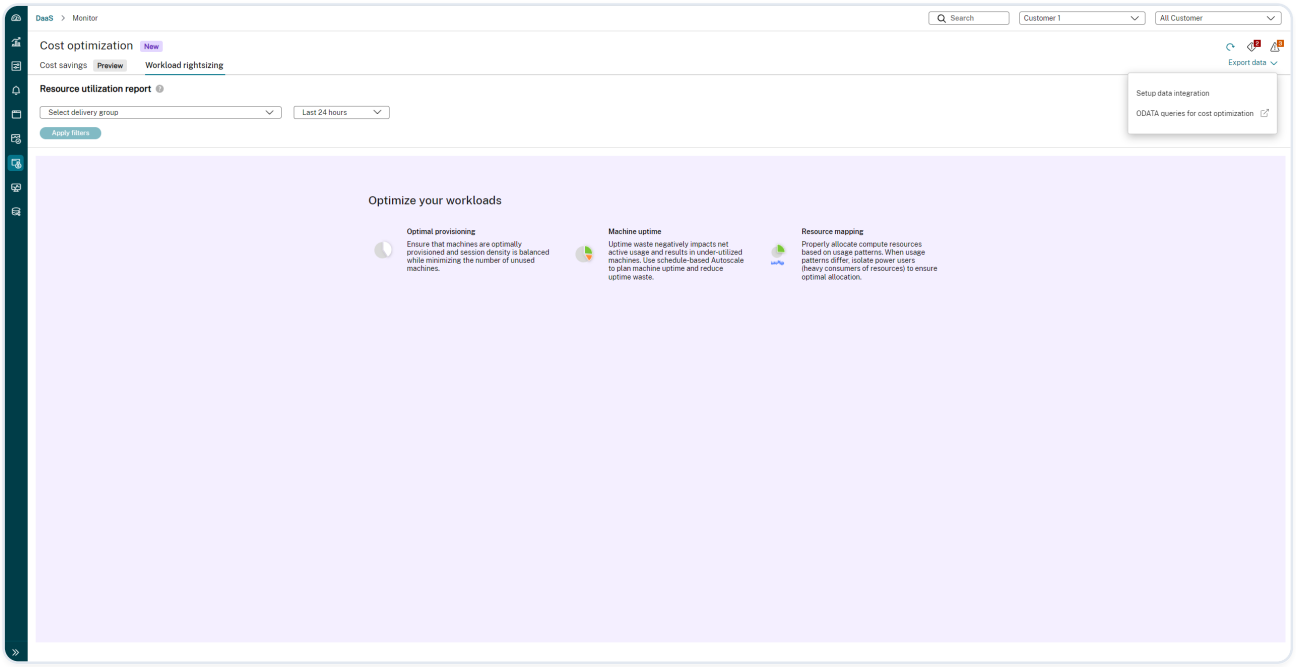
For other machines, cost is displayed based on the cost entered by admins in the Web Studio. If there is no cost mentioned in the Web Studio, the default cost of $1 is considered.

Export data

You can export the data on the **Cost optimization** page using data integration and ODATA queries. To export data, click **Export data** on the **Cost optimization** page, the following options are displayed:

- Setup data integration
- ODATA queries for cost optimization

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Setup data integration

You can integrate Cost optimization data with the Monitor Service API using which you can collect the data for troubleshooting and triaging the issues. For more information, see Integrations and data exports page.

ODATA queries for cost optimization

You can use the available sample ODATA queries on the **Cost optimization** page to export data.

Get started with ODATA

The following links help you to start using ODATA:

- Overview on ODATA
- Different methods to access Citrix Monitor Service data using the OData v4 endpoint in Citrix Cloud
- Use OData V4 aggregation queries in Citrix Monitor Service data
- How to connect PowerBI with DaaS Monitor using OData and API clients
- Get details of users with high logon duration using Postman
- How to Access the Monitor Service Data
- Data Access Protocol

Sample ODATA queries

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Find out unused VDA

To find out an unused VDA, you must provide a desktop group ID, start date, and end date of the VDA.

For more information to reduce spending on the unused resources, see Workload rightsizing.

Sample query:

```
https://api-us.cloud.com/monitorodata/ResourceUtilizationSummary?
$apply=filter(DesktopGroupId eq desktop-group-id and granularity eq 1440
and SummaryDate ge startdate and SummaryDate lt enddate)/
groupby((MachineId), aggregate(cast(TotalSessionCount, Edm.Int32) with
average as AvgTotalSessionCount))/filter(AvgTotalSessionCount eq 0.0)/
aggregate($count as UnusedVDACount)
```

FIND OUT THE DAILY AVERAGE UPTIME IN MINUTES

To find out the daily average uptime in minutes, you must provide the following:

- Desktop group ID
- Start date
- End date
- Day difference between the end date and start date.

For more information to reduce spending on the unused resources, see Workload rightsizing.

Sample query:

```
https://api-us.cloud.com/monitorodata/ResourceUtilizationSummary?
$apply=filter(desktopGroupId eq desktop-group-id and granularity eq 1440
and SummaryDate ge startdate and SummaryDate lt enddate)/
groupby((MachineId), aggregate(cast(UptimeInMinutes, Edm.Int32) div day-
difference with sum as TotalUptimeInMinutes))/
aggregate(TotalUptimeInMinutes with average as
DailyAverageUptimeInMinutes)
```

FIND OUT FAILED MACHINE POWER ACTION

For more information on failed machine power action, see Failed power on action and Failed Power off action.

Sample query:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
https://api-us.cloud.com/monitorodata/Machines?$filter=LifecycleState eq 0
and DesktopGroup/SessionSupport eq 1 and
(cast(LastPowerActionReason,'Edm.Int32') eq 6 or
cast(LastPowerActionReason,'Edm.Int32') eq 7 or
cast(LastPowerActionReason,'Edm.Int32') eq 8) and
(cast(LastPowerActionFailureReason,'Edm.Int32') eq 300 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 402 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 401) and MachineRole eq
0&$orderby=Name&$skip=0&$top=50&$expand=DesktopGroup($select=Name)&$select
=Sid,Id,Name,IsAssigned,IPAddress,FaultState,LastDeregisteredCode,FailureD
ate,CurrentPowerState,CurrentSessionCount,IsInMaintenanceMode,LastPowerAct
ionFailureReason,LastPowerActionCompletedDate
```

FIND OUT TOTAL SAVINGS

For more information on cost savings, see the Cost savings page.

Sample query:

```
https://api.cloud.com/monitorodata/MachineCostSavingsSummaries?
$apply=aggregate(TotalAmountSaved with sum as TotalAmountSavedSum)
```

FIND OUT THE MACHINE STATE

For more information on cost savings, see the Cost savings page.

Sample query:

```
https://api.cloud.com/monitorodata/MachineCostSavingsSummaries?
$filter=SummaryDate eq
2024-08-09T06:00:00Z&$select=TotalMachinesCount,PowerManagedMachinesOff,Po
werManagedMachinesInHibernate,PowerManagedMachinesOnWithSessions,PowerMana
gedMachinesOnWithoutSessions
```

Cost savings

The Cost savings page provides a visual representation of infrastructure savings accrued over a selected period and forecasts expected savings for the remaining days. By analyzing machine usage and sessions, this page helps you to identify achieved savings and opportunities for cost reduction. This page offers:

- Insight into the optimization of infrastructure costs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

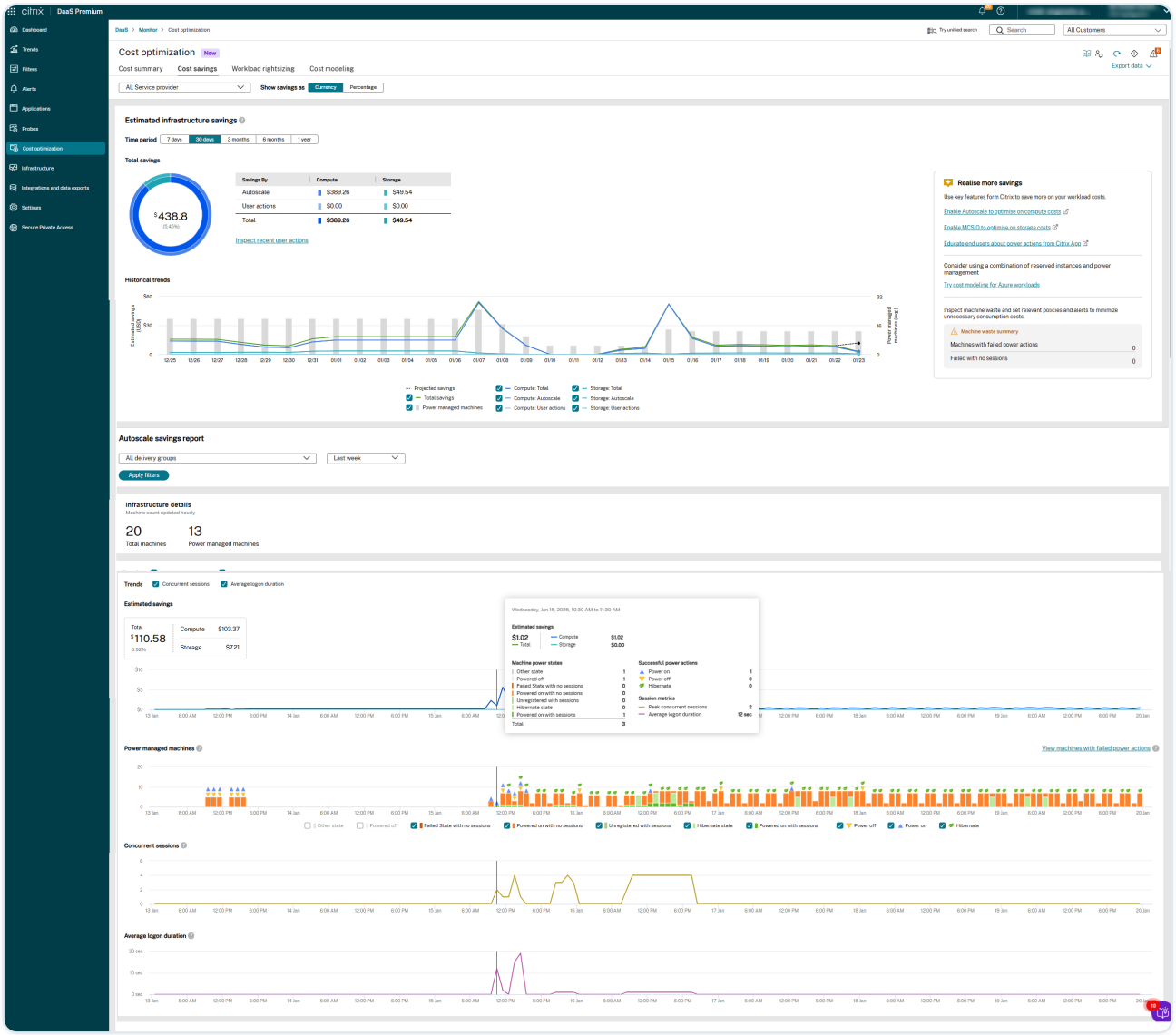
- The amount saved
- Information on a range of scenarios that might result in exceeding projected costs
- Potential opportunities for identification and strategic planning to realize infrastructure cost savings

The machine usage typically increases during peak hours, demanding increased resources. The Autoscale™ feature helps you to reduce cost by automatically powering off unused machines during the low demand period. The projected savings depend on this usage pattern. However, costs might exceed expectations under specific circumstances, such as when unused machines are present or when there are failures in Autoscale power actions. Identifying the reasons behind these occurrences was previously challenging.

The **Cost Optimization** page provides you detailed information on different scenarios that might cause you to exceed the expected cost. For example, if there are machines with no sessions, it shows you further opportunities for cost savings.

Click the **Cost Optimization** tab from the left menu on the **Home** page to access the **Cost Optimization** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



From the drop-down list on the top, if a site has both cloud and on-premises providers, you can now filter by all cloud providers, all on-premises providers, or individual providers.

Note:

The filter is applied immediately upon selection without an apply button.

The **Cost Optimization** page displays **Estimated infrastructure savings** and **Autoscale savings report**. You can view cost savings in the currency of the hypervisor or as a percentage of the incurred cost.

Estimated Infrastructure Savings: This graphical representation helps to evaluate the efficient utilization of infrastructure resources. This graph shows savings achieved from the compute-related savings and storage savings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

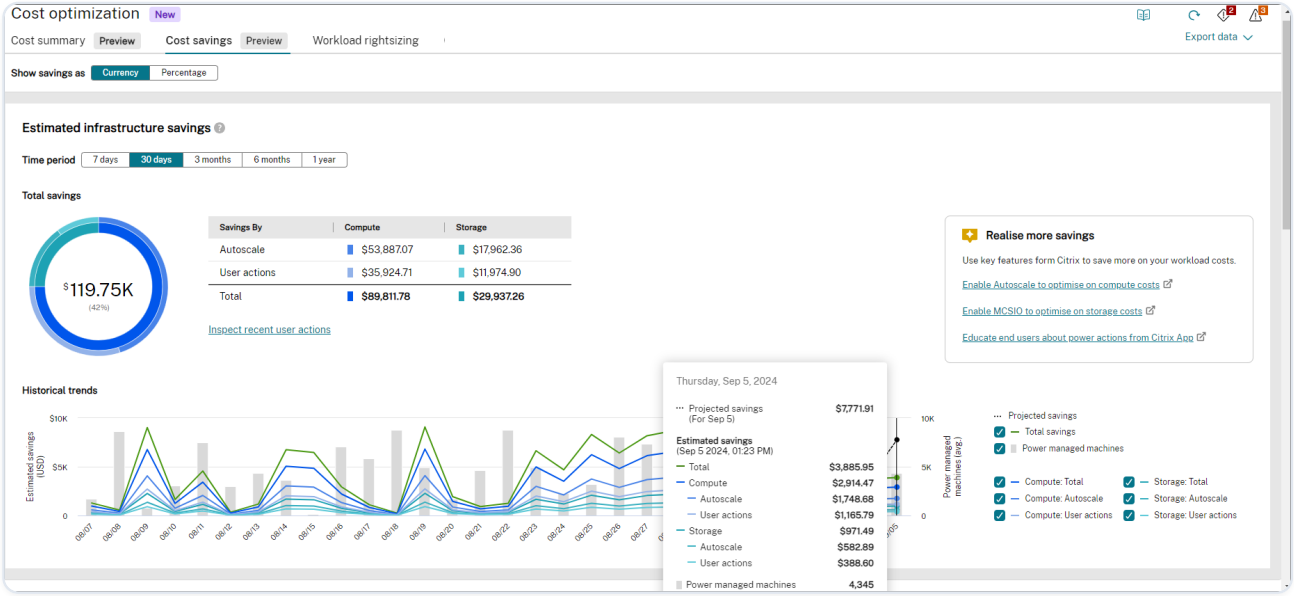
To view the savings from storage:

- Autoscale must be enabled to optimize compute costs. For more information, see Get started with Autoscale.
- Change the storage type to a lower tier when a VM is shut down to optimize storage costs. For more information, see Change the storage type to a lower tier when a VM is shut down documentation.
- This feature is currently applicable only to Azure machines.

You can view the results for the last:

- Seven days
- Thirty days
- Three months
- Six months
- Twelve months

The following picture shows the **Estimated infrastructure savings** section:



The following table lists the elements of Estimated savings graph:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELEMENT	DESCRIPTION
Total savings	Displays the total savings achieved in infrastructure for the selected duration. The savings are further categorized into storage and compute costs and are available in a tabular format.
Estimated savings	Displays the amount of savings achieved in infrastructure for the selected duration.
Power-managed machines	Displays the total number of power-managed machines.
Projected savings	Displays how much infrastructure savings can be done for the remaining duration.
Compute - Total	Displays total savings achieved from the compute-related savings.
Compute - Autoscale	Displays total savings achieved from the compute-related savings that are using the autoscale feature.
Compute - User actions	Displays total savings achieved from the compute-related savings that are from user actions.
Storage - Total	Displays total savings achieved from the storage savings.
Storage - Autoscale	Displays total savings achieved from the storage savings that are using the autoscale feature.
Storage - User action	Displays total savings achieved from the storage savings that are from user actions.

Autoscale Savings report: This graphical representation provides the savings report for the delivery groups for which the Autoscale feature is configured and enabled. This report is applicable only for the power-managed machines. You can select a delivery group and then select data for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

today, last day, last week, next week, this month, or next month. You can hover over any graphs to retrieve specific chart values.

NOTE:

If the delivery group is deleted, you can't get any data in the Autoscale savings report.

You can drill down to the following options from the delivery groups drop-down list :

- **All delivery groups**: Infrastructure details display all the delivery group information.
- **All single-session**: Infrastructure details for all delivery groups which are single-session machines along with the graphical representation of the machine power state, successful Autoscale power actions, and sessions when you hover over the chart.
- **All multi-session**: Infrastructure details for all delivery groups which are multi-session machines along with the graphical representation.
- **Select up to 15** - Infrastructure details display all the selected delivery groups, up to 15, along with a graphical representation.
- **Exclude up to 15** - Infrastructure details display all delivery groups, excluding the selected delivery groups, up to 15, with a graphical representation.

The data displays for the selected duration. The graphical representation of the **Estimated savings** is the actual savings of the selection made from the drop-down menu. When you hover over the peak points, the information about machine power state, successful Autoscale power actions, and sessions are shown.

Based on the delivery group selected, you can view the following details:

- **Infrastructure details**
  - Total machines and Power managed machines - Displays the total number of machines and out of that how many machines are power-managed. This data provides you a further opportunity to consider converting the remaining non-power managed machines to power-managed machines, thereby enabling the Autoscale feature for a more comprehensive coverage. The data in the Infrastructure details section shows the last known information updated every hour.
- **Catalog details**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Displays the name of the hypervisors (service providers). For more information, see Supported VDA hosting platforms. The data in the Catalog details shows the most recent data (live data) available at the current time.

You can get the following details:

- **Hypervisor name** - Displays the name of the hypervisor to which the site is connected. Displays all available hypervisors when multiple hypervisors are present.
- **Instance** - Displays the name of the instance.
- **Total cost per hour** - Displays the cost per machine per hour in the currency that the hypervisor supports. For Azure machines, when the Microsoft.Consumption/pricesheets/read permission is available, the effective price is displayed in the currency that is configured in the Azure subscription. If permissions aren't available, the Azure retail price is displayed. For more information, see Azure Retail Prices overview. For other machines, cost is displayed based on the cost entered by admins in the Web Studio. The default cost is $1 if the cost is not mentioned in Web Studio. For more information, see How is the cost calculated for optimizing the cost?.
- **Compute cost per hour** - Displays the cost savings from the compute-related savings.
- **Storage cost per hour** - Displays the cost savings from the storage savings.
- **Machines** - Displays the count of the machines for the selected instance.

- **Autoscale configuration (last known)**

  Tag in use - Displays the tag of the machines that is configured in the Autoscale settings in a WebStudio. You can also filter the data based on the tagged machines. In this case, you get only the tagged machines summary.

  Capacity buffer (peak) and **Capacity buffer (off peak)**

  Displays the percentage of buffer for machines that are powered on based on the maximum requirement of the delivery group during peak and off-peak times.

- **Estimated savings**

  Displays the amount of savings achieved in infrastructure for the selected duration. You can view the savings from compute-related savings and storage related savings for the Azure machines with Autoscale feature enabled.

- **Power managed machines**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With Autoscale enabled, the power-managed machines are turned off when not in use to optimize costs. You can get the following details:

- Number of machines powered off - This data helps you to analyze the number of machines that were powered off and thus helped to reduce cost.
- Hibernate state - This data helps you to analyze how many machines are in the hibernated state.
- Machines on with no sessions - This data provides you the opportunity to analyze why machines were active without any sessions and to plan for a more effective infrastructure savings strategy.
- Machines on with sessions - This data helps you to analyze the number of machines that were powered on and with active sessions.
- Power off - This data helps you to analyze the number of machines that were powered off or suspended and when this action was done. You can verify this data and make further modifications, contributing cost reduction.
- Power on - This data helps you to analyze how many machines were powered on and when this action was done. You can verify this data and make further modifications and thus help to reduce cost.
- Failed state with no sessions: This field displays the count of machines that are in a failed state and have no active sessions.
- Unregistered with sessions: This field displays the count of machines that are in an unregistered state but are still serving sessions.

NOTE:

You can see the count of machines in the Failed state with no sessions and Machines with failed power actions states and take actions based on the failure reason, time, and delivery group. The counts are clickable links that navigate to the Filters page for further actions. The count includes both single session and multi-session machines.

- **Concurrent sessions**

  Displays the total number of sessions at the selected time. This data helps you to determine when to power off machines for cost optimization.

- **Average logon duration**

Displays the average time for a user to log on over the selected time duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Workload rightsizing

The enhanced workload rightsizing page helps you analyze the usage and sizing aspects of your delivery groups. Hereby, delivery groups can be analyzed based on machine or user activity.

The machine-based analysis enables you to:

- Categorize virtual desktops based on usage to identify machines with no or low activity and reduce spending on unused resources.Usage Analysis
- Analyze resource utilization on virtual desktops to identify machines that needs to be right sized to reduce cost or improve user experience.Sizing Analysis

The user-based analysis enables you to:

- Categorize the users based on their activity. Consider removing the access entitlement of users with no activity for IT hygiene reasons. Users with low usage could be moved to shared resources for a more efficient use of resources.
- Analyze the resource consumption of users to identify cohorts with higher or lower than average resource consumption, and to distribute users more effectively.

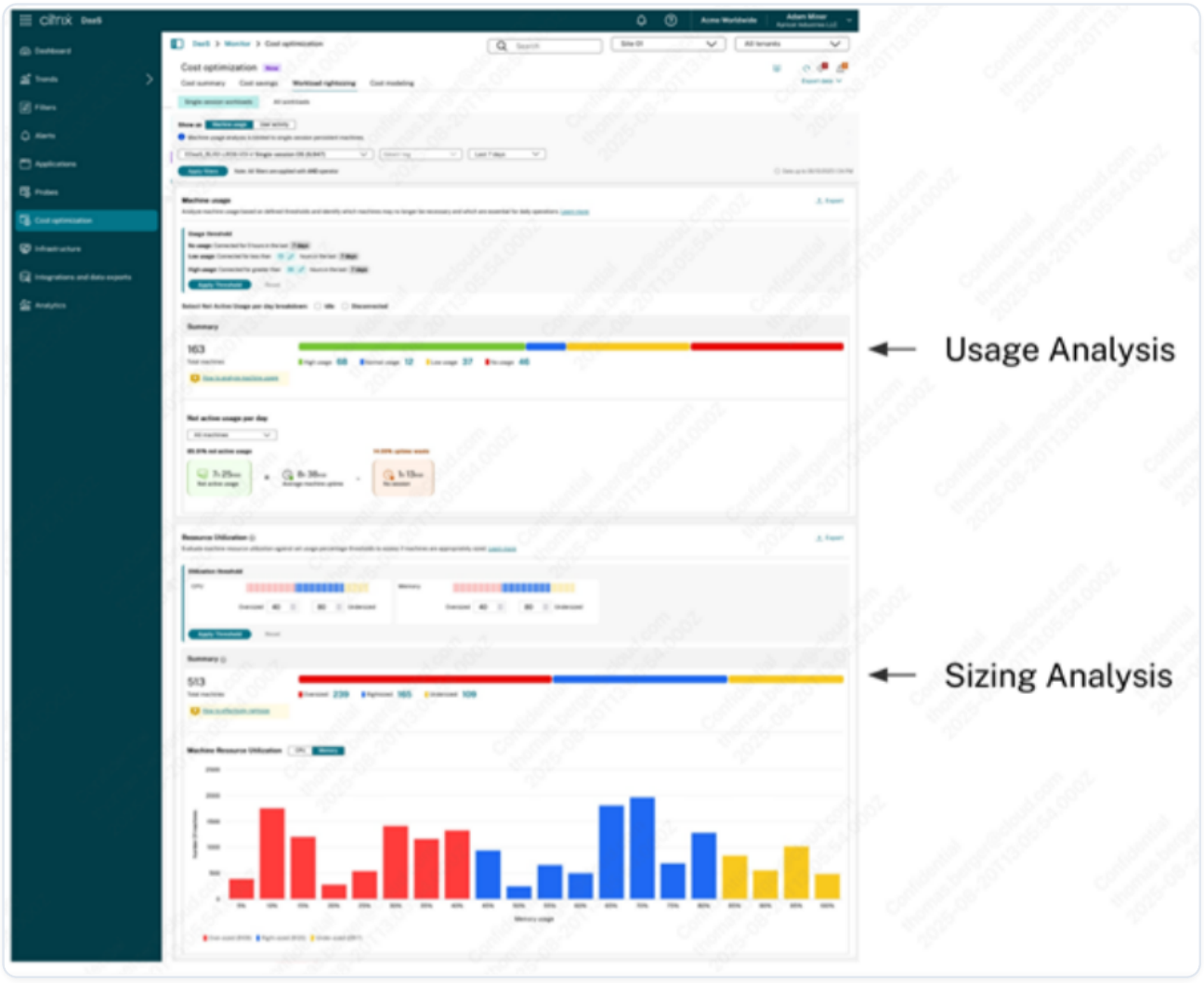
Click the **Cost Optimization** tab from the left menu on the Home page. And then, click the **Workload rightsizing** tab to access the **Workload rightsizing** page.

NOTE:

At the top of the page, you can toggle between machine and user-based analysis.

You can also click the **Rightsize this delivery group link** from the **Infrastructure details** section in the **Cost Optimization tab > Cost savings** to access the **Workload rightsizing** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Machine analysis is ideal for scenarios with virtual desktops statically assigned to users, such as Windows 365 Enterprise or Frontline dedicated. User analysis is useful for the analysis of delivery groups with randomly assigned virtual desktops. Both analyses are currently limited to single session machines.

NOTE:

The classic rightsizing analysis, accessible through the “All Workloads” button at the top of the page, will be deprecated in an upcoming release.

Usage analysis

Usage analysis enables you to categorize virtual desktops based on their activity levels as follows:

- **Low or no usage machines (Dedicated machines)**: Machines in this category might no longer be necessary and can potentially be removed to save costs.
- **High usage machines (Dedicated machines)**: This category is critical for daily operations and might require additional service continuity measures.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Low or no-usage users (Pooled machines)**: Users with no activity within the selected timeframe may no longer need to be assigned to the delivery group. Removing them can help reduce the costs of your environment. Low-activity users may benefit from reassignment. To consolidate usage and reduce costs, consider moving low-activity users who have a dedicated desktop to a pooled desktop.

To perform usage analysis:

1. Select machines based on Delivery Groups or Tags
2. Choose the timeframe for analysis.
3. Review and configure thresholds that define low and high usage patterns.
4. Examine the summary section showing virtual desktop categorization based on configured thresholds.
5. Review the net active usage section displaying usage details for each machine. Idle and disconnected time can be included or excluded in net active usage analysis.
6. Use the drop-down to focus on specific categories.
7. Export machine names and associated users using the export function to review the names of the machines and their associated users.

NOTE:

The example provided illustrates machine-based usage analysis; however, the steps for user-based analysis are equivalent and are not discussed separately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Sizing analysis

Sizing analysis categorizes virtual desktops or users based on resource utilization as follows:

- Oversized machines: Have more resources than necessary; reducing resource allocation can lower costs without impacting user experience
- Undersized machines: Lack sufficient resources; user experience can be improved by allocating more resources
- Right-sized machines: Fall between the oversized and undersized thresholds
- Light users: These users may benefit from reassignment. To consolidate and reduce costs, consider moving light users with a dedicated desktop to a shared pooled desktop.
- Moderate users: Moderate users are properly assigned to machines in a delivery group and should expect an optimal user experience.
- Power users: Power users consume significant resources, and when they share a pooled desktop, their high usage can negatively impact the overall experience for other users on that machine. To enhance the experience for all users and ensure that power users have consistent access to a desktop, consider moving these users to a dedicated desktop or assigning them to individual delivery groups.

To perform Sizing Analysis:

1. Select machines based on Delivery Groups or Tags
2. Choose the timeframe for analysis.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Configure separate thresholds for CPU and Memory utilization.
4. Review the summary section showing virtual desktop categorization
5. Analyze the machine resource utilization chart showing CPU and Memory distribution
6. Fine-tune machine configurations based on resource type and identify outliers
7. Export machine names and associated users using the export function to review the names of the machines and their associated users

NOTE:

The example provided illustrates machine-based resource consumption analysis; however, the steps for user-based analysis are equivalent and are not discussed separately.



NOTE:

The utilization analysis uses 95th-percentile utilization for delivery groups in the selected timeframe, indicating that 95% of CPU or Memory utilization is at or below the set value.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Best practices

- Use usage analysis to identify cost-saving opportunities by removing underutilized machines.
- Apply sizing analysis to optimize resource allocation and improve user experience.
- Use machine analysis for statically assigned virtual desktop scenarios for accurate analysis.
- Use user activity for pooled virtual desktop scenarios for accurate analysis.
- Consider roaming patterns when analyzing randomly assigned virtual desktops.
- Export detailed reports for further analysis and documentation.

Key terms and charts

Machine net active usage: Net active usage is calculated by deducting the total uptime waste from the average machine uptime. All times are in minutes.

Percentage of Net Active Usage: The actual time users actively used the machine. This is the duration when at least one session was active while the machine was powered on.

Average Machine Uptime: The total time the machine was powered on.

No Session: The wasted uptime due to no active sessions.

Idle Time: Wasted uptime due to idle sessions. This is the time when all sessions on the machine are idle.

Disconnected Time: Wasted uptime due to disconnected sessions. This is the time when all sessions on the machine are disconnected.

Total machine - Displays the total number of machines. This includes all the machines which were powered on during the selected period.

Average session density - This is an average across the number of machines and across the selected time period. Refers to the amount of session load on a machine which affects the resource available for sessions.

Unused machines - Displays the number of machines which had no sessions over the selected time period but which were still powered on.

CPU utilization:

Machine cohort - Provides information about the machine groups categorized into top, middle, and bottom based on its CPU utilization. Thresholds limit can be configured by the admins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Range of CPU Peaks - Displays the CPU peaks range based on its utilization corresponding to the machine cohort.

Machines - Displays the number of machines corresponding to the machine cohort.

Session density - Displays the session density corresponding to the machine cohort.

Resource utilization trends:

Range of CPU peaks - Displays the range of CPU peaks in a band. When you hover on any point in the band, the top and bottom value of the band is displayed.

Peak memory utilization - Displays the highest memory utilization for the selected machines and for the selected time over a graph.

Average Session density - Displays the average session density for the selected machines and for the selected time over a graph.

Average ICA RTT - Displays the average round trip time for the session. This chart shows breaks when there are no active sessions or when sessions are disconnected.

Average logon duration - Displays the average logon duration for the selected machines and for the selected time period over a graph. This chart shows data when a new logon starts during the selected time.

Cost summary

The **Cost summary** page provides a comprehensive summary of the expenses associated with running the Citrix® environment. With this enhancement, you gain visibility into:

- The overall cost per user
- Cost of delivering virtualization by the chosen Workload providers, desktop types, and VM series sets

This page offers:

- Insight into the cost of delivering a virtualized app or desktop to a user
- The amount saved
- Information on costs and savings categorized by:
    - Platform provider
    - OS type

© 1997–2026 Citrix Systems, Inc. All rights reserved.

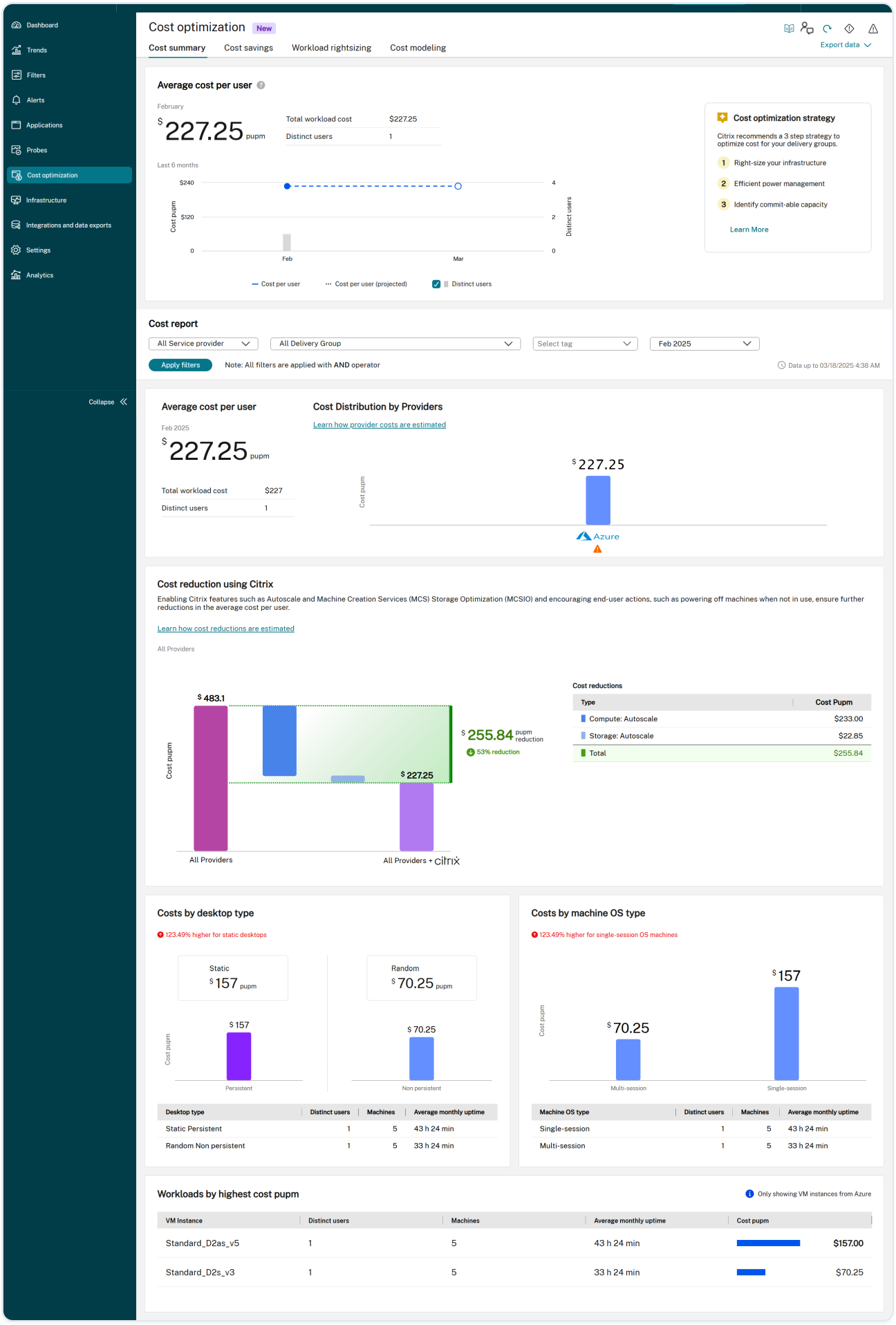
- Desktop type
- VM series

NOTE:

The **Cost summary** page is available only if the site has been running for at least 15 days in a month.

To access the **Cost summary** page, click **Monitor** > **Cost optimization** > **Cost summary**. The **Cost summary** page appears:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Cost summary** page includes:

- **Average cost per user**

  You can view the actual cost per user per month for the last six months and also the projected cost for the current month. In addition, you can see the total cost of workloads and the number of distinct users on the site. When multiple currencies are involved, costs are displayed in USD if USD is one of them. Otherwise, the cost is shown in a randomly selected currency from the list. The cost savings compared to the last and last to the last months are provided in percentage. Also, the changes in the number of distinct users are also presented. The graphical representation shows the trend for every month.

  You can use the average cost per user and optimize the usage.

- **Cost report**

  You can view the cost report of the selected service providers, for the selected delivery group, and for the selected tag. You can view the report for the last three months separately or a consolidated view of the last three months' data.

- **Cost reduction using Citrix**

  You can further reduce the average cost per user by enabling Citrix features such as Autoscale and Machine Creation Services™ (MCS), Storage Optimization (MCSIO). Also, encourage end-user actions, such as powering off machines when not in use.

  This data displays the total savings when Citrix features are applied. It also displays the savings from the end-user actions.

- **Cost by desktop type**

  You can view the costs of the following types of desktops:

  - **Static persistent:** The user signs on to the same virtual desktop each time and the changes made to the desktop are saved.
  - **Static non-persistent:** The user signs on to the same virtual desktop each time and the changes made to the desktop are not saved.
  - **Random persistent:** The user is assigned a virtual desktop from the pool of desktops and the changes made to the desktop are saved.
  - **Random non-persistent:** The user is assigned a virtual desktop from the pool of desktops and the changes made to the desktop are not saved.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can view the number of distinct users, machines, and average monthly uptime for each type of machine.

You can use this data and plan for saving costs by moving users to different types of desktops. For example, static persistent desktop types require more resource usage compared to random non-persistent desktops. So, you can plan to move some users from static persistent desktop types to random non-persistent desktop types.

- **Cost by OS type**

  You can view the costs of single-session and multi-session OS types. You can view the machine OS type, distinct users, machines, and average monthly uptime. You can use this data and plan for saving costs by moving users to different types of OS.

- **Workloads by highest cost per user per month**

  You can view the details of the highest cost per user per month, including the virtual machine instance, number of distinct users, and average uptime of the machine. Also, you can see the number of machines and the cost per user.

  Use this data to view the cost for each VM configuration type and decide which configurations to assign to users.

Cost modeling

The new cost modeling feature supports Azure workloads and provides recommendations based on usage patterns. Customers receive recommendations on whether Azure Reservations or Savings Plan is more suitable to provide maximum cost savings. Azure Reservations customers reserve a specific number of machines upfront at a discounted flat cost, while savings plans allow them to commit to a dollar amount for discounted rates. The feature analyzes the last 28 days of data to provide estimated recommendations. This helps customers save costs by making informed decisions on resource allocation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- For optimal estimates, it is recommended to use data from a stable environment over the last 28 days. Avoid using data from periods of unusual activity, such as vacations or sudden spikes in usage. Wait until your usage returns to baseline levels before taking these recommendations.
- Cost modeling is designed for cloud-based workloads with flexible pricing. For workloads with fixed monthly pricing or for on-premises workloads, use Workload Rightsizing instead.

Benefits:

- Provides tailored cost-saving recommendations.
- Supports both reservation and savings plans.
- Analyzes recent usage data for accurate insights.
- Helps optimize resource allocation and reduce expenses.
- Offers flexibility in selecting delivery groups, tags, VM series, and regions.

NOTE:

Cost modeling is supported only for Azure workloads.

Types of plans

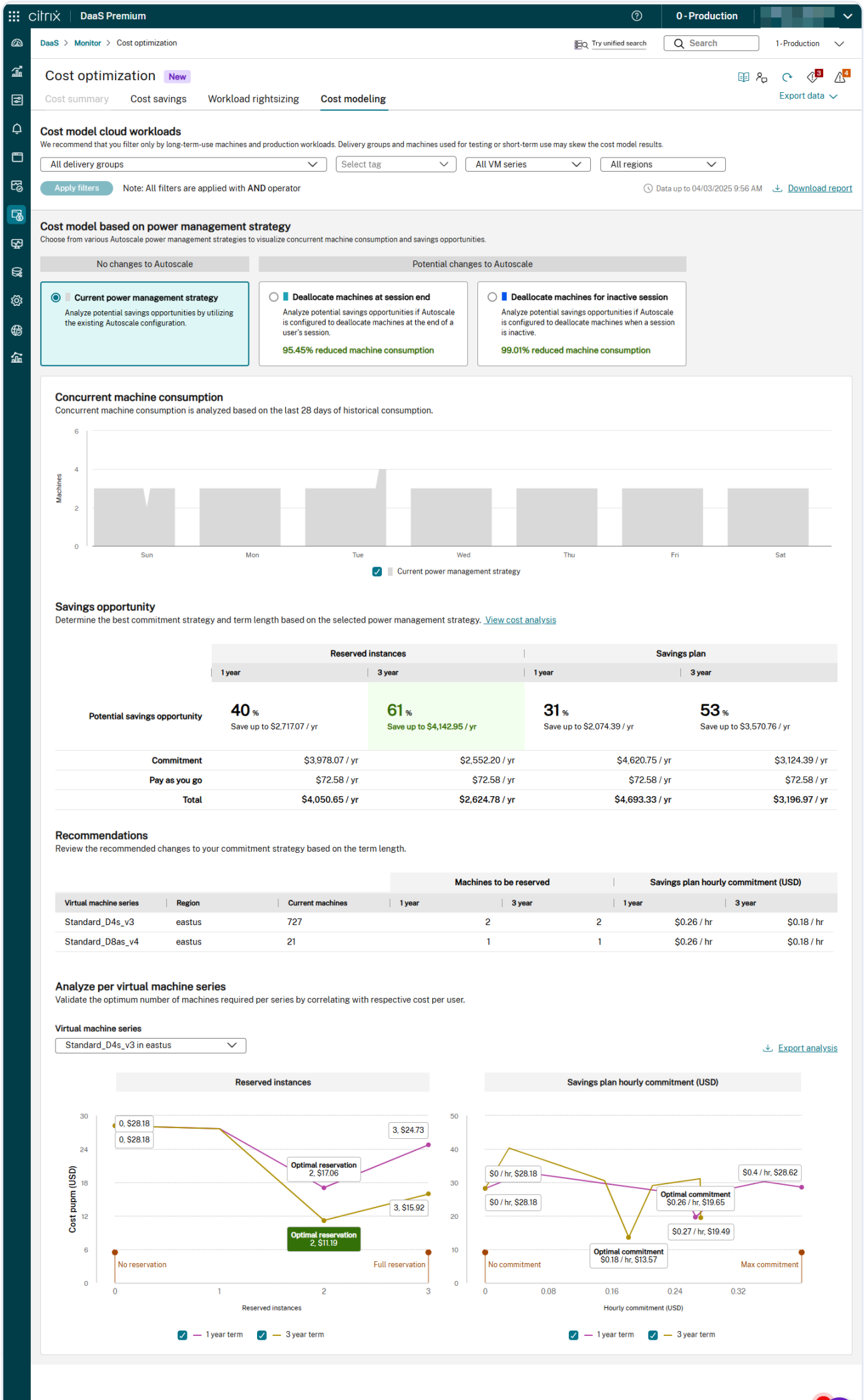
In Azure, there are two types of plans to save costs:

- **Azure Reservations**: Customers decide how many machines to reserve upfront. Reservation has a different flat cost at a discounted rate compared to the pay-as-you-go cost.
- **Savings Plan**: Customers commit to a specific dollar amount rather than a number of machines. Up until that amount is consumed, they are charged a discounted cost. After that, they pay the pay-as-you-go cost.

The **Cost modeling** page provides recommendations for each plan independently, showing potential savings.

Click **Cost optimization > Cost modeling**. The **Cost model and Cloud workloads** page appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


citrix | DaaS Premium
0 - Production
DaaS > Monitor > Cost optimization
Try unified search
Search
1 - Production
Cost optimization New
Cost summary
Cost savings
Workload rightsizing
Cost modeling
Export data
Cost model cloud workloads
We recommend that you filter only by long-term-use machines and production workloads. Delivery groups and machines used for testing or short-term use may skew the cost model results.
All delivery groups
Select tag
All VM series
All regions
Apply filters
Note: All filters are applied with AND operator
Data up to 04/03/2025 9:56 AM
Download report
Cost model based on power management strategy
Choose from various Autoscale power management strategies to visualize concurrent machine consumption and savings opportunities.
No changes to Autoscale
Potential changes to Autoscale
Current power management strategy
Analyze potential savings opportunities by utilizing the existing Autoscale configuration.
Deallocate machines at session end
Analyze potential savings opportunities if Autoscale is configured to deallocate machines at the end of a user's session.
95.45% reduced machine consumption
Deallocate machines for inactive session
Analyze potential savings opportunities if Autoscale is configured to deallocate machines when a session is inactive.
99.01% reduced machine consumption
Concurrent machine consumption
Concurrent machine consumption is analyzed based on the last 28 days of historical consumption.
Machines
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Current power management strategy
Savings opportunity
Determine the best commitment strategy and term length based on the selected power management strategy. View cost analysis
Reserved instances
Savings plan
1 year
3 year
Potential savings opportunity
40 %
Save up to $2,717.07 / yr
61 %
Save up to $4,142.95 / yr
31 %
Save up to $2,074.39 / yr
53 %
Save up to $3,570.76 / yr
Commitment
$3,978.07 / yr
$2,552.20 / yr
$4,620.75 / yr
$3,124.39 / yr
Pay as you go
$72.58 / yr
$72.58 / yr
$72.58 / yr
$72.58 / yr
Total
$4,050.65 / yr
$2,624.78 / yr
$4,693.33 / yr
$3,196.97 / yr
Recommendations
Review the recommended changes to your commitment strategy based on the term length.
Machines to be reserved
Savings plan hourly commitment (USD)
Virtual machine series
Region
Current machines
1 year
3 year
Standard_D4s_v3
eastus
727
2
2
$0.26 / hr
$0.18 / hr
Standard_D8as_v4
eastus
21
1
1
$0.26 / hr
$0.18 / hr
Analyze per virtual machine series
Validate the optimum number of machines required per series by correlating with respective cost per user.
Virtual machine series
Standard_D4s_v3 in eastus
Export analysis
Reserved instances
Savings plan hourly commitment (USD)
Cost pupm (USD)
0, $28.18
0, $28.18
3, $24.73
Optimal reservation
2, $17.06
3, $15.92
Optimal reservation
2, $11.19
No reservation
Full reservation
Reserved instances
$0 / hr, $28.18
$0 / hr, $28.18
$0.4 / hr, $28.62
Optimal commitment
$0.26 / hr, $19.65
$0.27 / hr, $19.49
Optimal commitment
$0.18 / hr, $13.57
No commitment
Max commitment
Hourly commitment (USD)
1 year term
3 year term
1 year term
3 year term

You can select all delivery groups, up to 15 (or the actual count) delivery groups, and exclude up to 15 (or the actual count) delivery groups if needed. You can select **All single-session** or **All multi-session** from drop-down lists. You can also filter by **Tags**, **VM series**, and **Regions**. If you do not select any options, the analysis runs on the entire applicable data set by default, considering the last 28 days of data.

NOTE:

The cost modeling recommendation is based on data from the last 28 days and assumes that the behavior during this period remains consistent.

Power management strategies

The data analysis varies based on the selected power management strategy. You can select one of the following Autoscale™ power management strategies to visualize the concurrent machine consumption and savings opportunities:

- **Current power management strategy**: Select this strategy to analyze potential savings using the existing Autoscale configuration. There is no change to the Autoscale configuration. The recommended cost modeling is generated based on the current Autoscale setup, calculating costs for all machines that are up and running.
- **Deallocate machines at session end**: Select this strategy if you are willing to change the Autoscale configuration to deallocate machines at the end of user sessions to analyze potential savings. The recommended cost modeling is generated based on the updated Autoscale configuration, calculating costs only for active session time, ignoring disconnect time.
- **Deallocate machines for inactive session**: Select this strategy if you are willing to change the Autoscale configuration to deallocate machines when sessions are inactive to analyze potential savings. The recommended cost modeling is generated based on the updated Autoscale configuration, calculating costs only for the time when sessions are active and not idle.

For example, if the machine is up for 60 minutes and the session is disconnected for 20 minutes, the remaining 40 minutes is the active session time. If the user is idle for 10 minutes during the active session, the net usage is only 30 minutes.

- In the **Current power management strategy**, the net usage is 60 minutes.
- In the **Deallocate machines at session end strategy**, the net usage, excluding disconnect time, is 40 minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In the **Deallocate machines for inactive session strategy**, including idle time, the net usage is 30 minutes.

These criteria serve as the baseline for analysis. These strategies help determine the net usage of machines more accurately.

Machine consumption and recommendations

The **Cost modeling**page provides the following details on the machine consumption and recommendations:

- **Concurrent machine consumption graph**: This graph displays the baseline usage over the last 28 days, with each bar representing one day of the week. The baseline is calculated using the 75th percentile (p75) of usage, an aggregation metric similar to average or median. For example, for each day and hour, such as Tuesday at 10 AM, the baseline is determined by analyzing the p75 of data from the previous four Tuesdays at 10 AM. This process is repeated for all hours and days of the week. Hover over the graph to view the number of machines consumed under the current power management strategy and the selected strategy when potential changes to Autoscale are applied.
- **Savings opportunity**: View the potential savings opportunities for both Azure Reservations and Savings Plans for one-year and three-year terms. The savings opportunity for **Commitment** and **Pay-as-you-go** options is displayed.
- **Recommendations**: View the recommended changes to both Azure Reservations and Savings Plans. The recommendations include commitments for each plan for all applicable combinations of virtual machine series, types, and regions. Data is available for one-year and three-year terms.

Analyze per virtual machine series

Select the virtual machine series from the drop-down list to validate the optimum number of machines with respect to cost per user. The cost per user per month is an estimate of the projected monthly cost per user. This estimate helps customers understand the projected monthly cost per user if they reserve a specific number of machines under Azure Reservations or commit to a specific hourly dollar amount under the **Savings Plan**. View the cost per user for Azure Reserved Instances and Savings Plan hourly commitments. The graph displays data points for various reservation levels (ranging from **No Reservation** to **Full Reservation**, including **Optimal Reservation**) and hourly cost commitment levels (ranging from **No Commitment** to **Max Commitment**, including **Optimal Commitment**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Cost modeling** page provides valuable insights and recommendations to help customers optimize their Azure workloads and save costs. By analyzing usage patterns and selecting the appropriate plan, customers can achieve significant savings.

Feature compatibility matrix

Citrix Monitor supports three Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) editions. They are **Platinum**, **Citrix DaaS Advanced**, and **Citrix DaaS Advanced Plus**. Specific Citrix Monitor features, VDA versions, dependent components, and their respective license editions are listed in the following table.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Multi-select support for delivery groups	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Improved handling of vertical and horizontal load balancing alerts	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Enhanced network metrics collection for session troubleshooting	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Observability for multi-session VDA	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Cost summary	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Monitoring VDA logon duration details	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Bulk alert dismissal	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Enhanced network metrics monitoring in Citrix Monitor.	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Cost modeling for Azure workloads	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Option to extend monitoring of HDX optimization beyond Microsoft Teams	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
New metrics in the Monitor dashboard such as "Total connected users" and "Citrix Workspace app versions found in your environment"	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Enhancements to Cost savings page	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Connector Appliance health metrics	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Improvement to Workload rightsizing	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Enhancement to Session Performance tab	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Cost Savings by optimizing storage usage	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Monitor action enhancements	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Option to view and troubleshoot Secure Private Access Sessions for hybrid deployments	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Integration with Webhook	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Least used and unused published apps report	VDA 7 2212 running 64-bit Windows	Yes	No	No
Monitor and troubleshoot Secure Private Access	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Secure Private Access tab on Monitor	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Visibility for Secure Private Access Service	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Enhancement to Connections tab	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Machine net active usage	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Cloud Connector health metrics	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Displaying policy details in Device Posture Events	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Enhancement to Trends page	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Export data	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Webhook configuration using PowerShell SDK	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Application usage monitoring charts on Dashboard	VDA 7 2212 running 64-bit Windows	Yes	No	No
Integrations and data exports	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Enhancement on triaging user profile load issues	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Advanced alert policies	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Enhancements on alert content	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Local Host Cache config sync failure alert monitoring	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Failed power on action and Failed Power off action alert	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Infrastructure policy (Preview)	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Infrastructure monitoring (Preview)	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Options to troubleshoot when ICA RTT or Session Logon Duration data fails to populate	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Enhancement to Cost savings page	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Diagnose historical user sessions (Preview)	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Machine uptime alert	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Workload rightsizing	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Local Host Cache activity dashboard	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Enhanced Performance Metrics panel	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Improved Session Logon view	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Unregistered Machines (in %)	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Cost Optimization	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Inspect machines with recent power actions	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Support for Microsoft Teams version 2.1 or earlier	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Support for HDX Plus for Windows 365 Cloud PCs and Azure Virtual Desktops	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Summary of the Probe Metrics and the Probe Failure Stages	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
End-to-end Network Hop view	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Play back live and recorded sessions	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Microsoft Teams Optimization	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Send Message progress	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Citrix Probe Agent authentication support via Citrix Gateway with domain credentials and Multi-factor authentication	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Session Topology	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Trends for Session	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Performance metrics				
Monitor multiple Citrix DaaS instances (Preview)	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
View endpoint device status in Session Launch Diagnostics using Device Posture	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Failed Machines alert	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Search Session Diagnostics with user name	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Real-time GPU Utilization available for AMD GPUs	VDA 7 2212 running 64-bit Windows	Yes	Yes	Yes
Access Citrix Analytics for Performance-Session Details	Citrix Analytics for Performance entitlement	Yes	Yes	Yes
Session Auto Reconnect	VDA 1906	Yes	Yes	Yes
Session Startup Duration	VDA 1903	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Desktop Probing	Citrix Probe Agent 1903	Yes	No	No
Citrix Profile Management Duration in Profile Load	VDA 1903	Yes	Yes	Yes
Profile Drilldown	VDA 1811	Yes	Yes	Yes
Hypervisor Alerts Monitoring	None	Yes	No	No
Application Probing	Citrix Application Probe Agent 1811	Yes	No	No
Microsoft RDS License Health	VDA 7.16	Yes	Yes	Yes
Access to machine console from Monitor	XenServer Hypervisor 7.3	Yes	Yes	Yes
Export of Filters Data	None	Yes	Yes	Yes
Interactive Session Drill Down	VDA 1808	Yes	Yes	Yes
GPO Drill Down	VDA 1808	Yes	Yes	Yes
Machine Historical Data	None	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Available Using OData API				
Smart Alert Policies	None	Yes	No	No
Health Assistant Link	None	Yes	Yes	Yes
Interactive Session Drill-down	None	Yes	Yes	Yes
Application Analytics	VDA 7.15	Yes	Yes	Yes
OData API V.4	None	Yes	Yes	Yes
Shadow Linux VDA Users	VDA 7.16	Yes	Yes	Yes
Machine Console Access	None	Yes	Yes	Yes
Application Failure Monitoring	VDA 7.15	Yes	Yes	Yes
Application-centric Troubleshooting	VDA 7.13	Yes	Yes	Yes
Disk Monitoring	VDA 7.14	Yes	Yes	Yes
GPU Monitoring	VDA 7.14	Yes	Yes	Yes
Transport Protocol on	VDA 7.13	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Session Details Panel				
User-friendly Connection and Machine Failure Descriptions	VDA 7.x	Yes	Yes	Yes
Historical Data Retention	VDA 7.x	Yes	No	No
Custom Reporting	VDA 7.x	Yes	No	No
Resource Utilization Reporting	VDA 7.11	Yes	Yes	Yes
Alerting Extended for CPU, Memory and ICA RTT Conditions	VDA 7.11	Yes	No	No
Export Report Improvements	VDA 7.x	Yes	Yes	Yes
Logon Duration Breakdown	VDA 7.x	Yes	Yes	Yes
Proactive Monitoring and Alerting	VDA 7.x	Yes	No	No
Hosted Applications Usage	VDA 7.x	Yes	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DEPENDENCIES - MIN VERSION REQUIRED	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Single-session and Multi-session OS Usage	VDA 7.x	Yes	No	No
Support for Framehawk Virtual Channel	VDA 7.6	Yes	Yes	Yes

Aggregated Search across multiple DaaS instances

Citrix DaaS allows customers to aggregate multiple instances of their Citrix DaaS service using a hub and spoke model. With this configuration, you can use the universal search feature to search for users, machines, endpoints and transactions across all the aggregated DaaS tenants.

Pre-requisites

All the DaaS tenants must be aggregated using a hub and spoke topology. For more information regarding the configuration required to aggregate the spoke service instances to a hub, see Aggregate multiple Citrix DaaS instances.

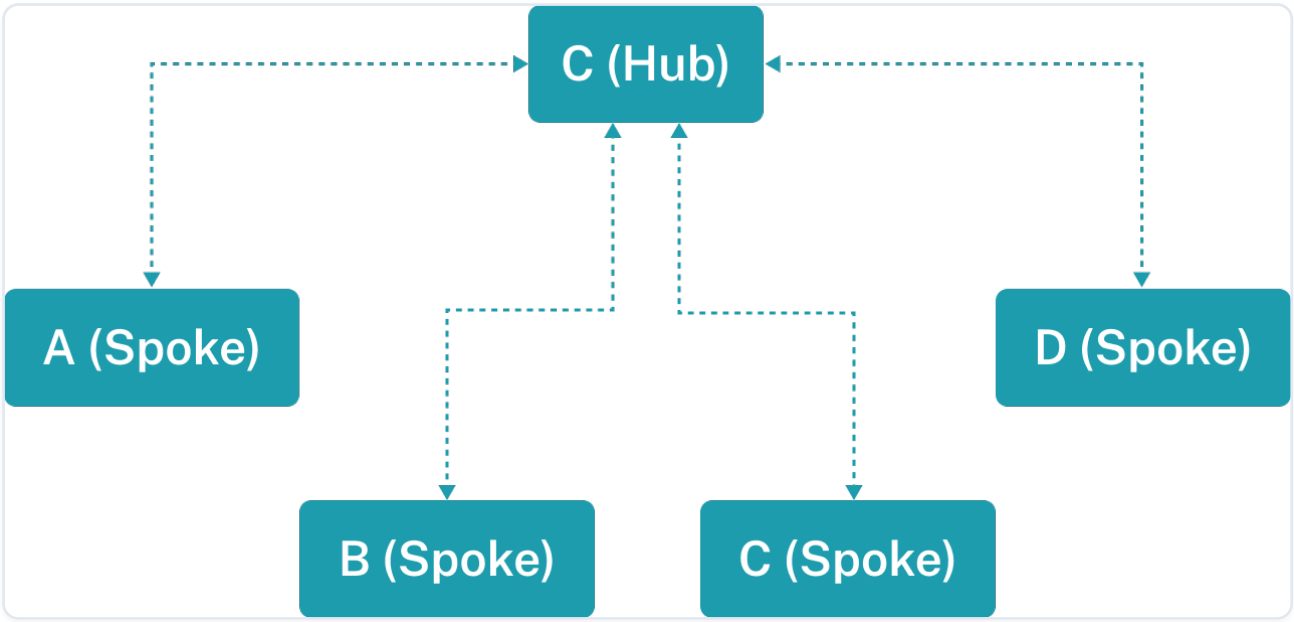
NOTE:

Monitor supports aggregation of up to four DaaS orgIDs (spokes) under a single orgID (hub), allowing a total of 5 DaaS instances to be monitored together.

How it works

Once the hub and spoke configuration of DaaS tenants is completed, administrators can log into the Monitor console of their configured hub instance to search for users, machines, endpoints, and transactions. The search aggregates results from the hub and all its spokes, rendering results for further troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In case bidirectional enumeration of the hub and spoke instances is configured, administrators can log into the hub or any of the spokes to perform the search.

Delegated administration

Delegated administration uses three concepts: administrators, roles, and scopes. Permissions are based on an administrator's role and the scope of this role. For example, an administrator might be assigned a Help Desk administrator role where the scope involves responsibility for end-users at one site only.

Administrative permissions determine the monitoring interface presented to administrators and the tasks they can perform. Permissions determine:

- The views the administrator can access, collectively referred to as a view.
- The desktops, machines, and sessions that the administrator can view and interact with.
- The commands the administrator can perform, such as shadowing a user's session or enabling maintenance mode.

Monitoring now supports delegated administrator roles that allow you to assign custom defined or built-in roles to administrators. The role determines the available permissions and hence, how an administrator uses monitoring. You can also define the scope applicable for those roles. The scope defines the objects for which the role is applicable.

For information about creating delegated administrators, see the main Delegated administration article.

The built-in roles and permissions determine how administrators use **Monitor**:

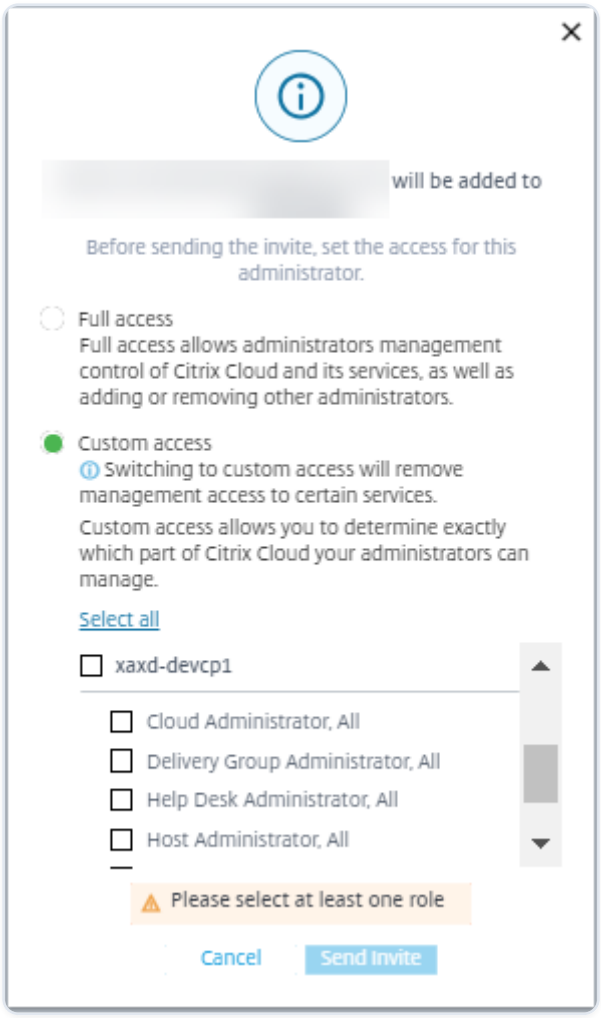
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ADMINISTRATOR ROLE	PERMISSIONS IN MONITOR
Full Administrator	Full access to all views and can perform all commands, including shadowing a user's session, enabling maintenance mode, and exporting trends data.
Delivery group Administrator	Full access to all views and can perform all commands, including shadowing a user's session, enabling maintenance mode, and exporting trends data.
Read Only Administrator	Can access all views and see all objects in specified scopes in addition to global information. Can download reports from HDX™ channels and can export Trends data using the Export option in the Trends view. Cannot perform any other commands or change anything in the views.
Help Desk Administrator	Can access only the Help Desk and User Details views and can view only objects that the administrator is delegated to manage. Can shadow a user’s session and perform commands for that user. Can perform maintenance mode operations. Can use power control options for Single session OS Machines. Can perform Build-In Scripted Task. Can perform Custom Scripted Task. Cannot access the Dashboard, Trends, Alerts, or Filters views. Cannot use power control options for Multi-session OS machines.
Machine catalog Administrator	Can access only the Machine Details page (Machine-based search).
Host Administrator	No access. This administrator is not supported for Monitor and cannot view data.
Probe Agent Administrator	Read-only access to Applications page, cannot access any other view. Meant to run the Citrix Probe Agent on endpoint machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ADMINISTRATOR ROLE	PERMISSIONS IN MONITOR
Monitoring Full Administrator	Has full access to all views and commands in the **Monitor** console.
Session Administrator	Can view Delivery Groups and manage their associated sessions and machines on the **Filters** page of the **Monitor** console.

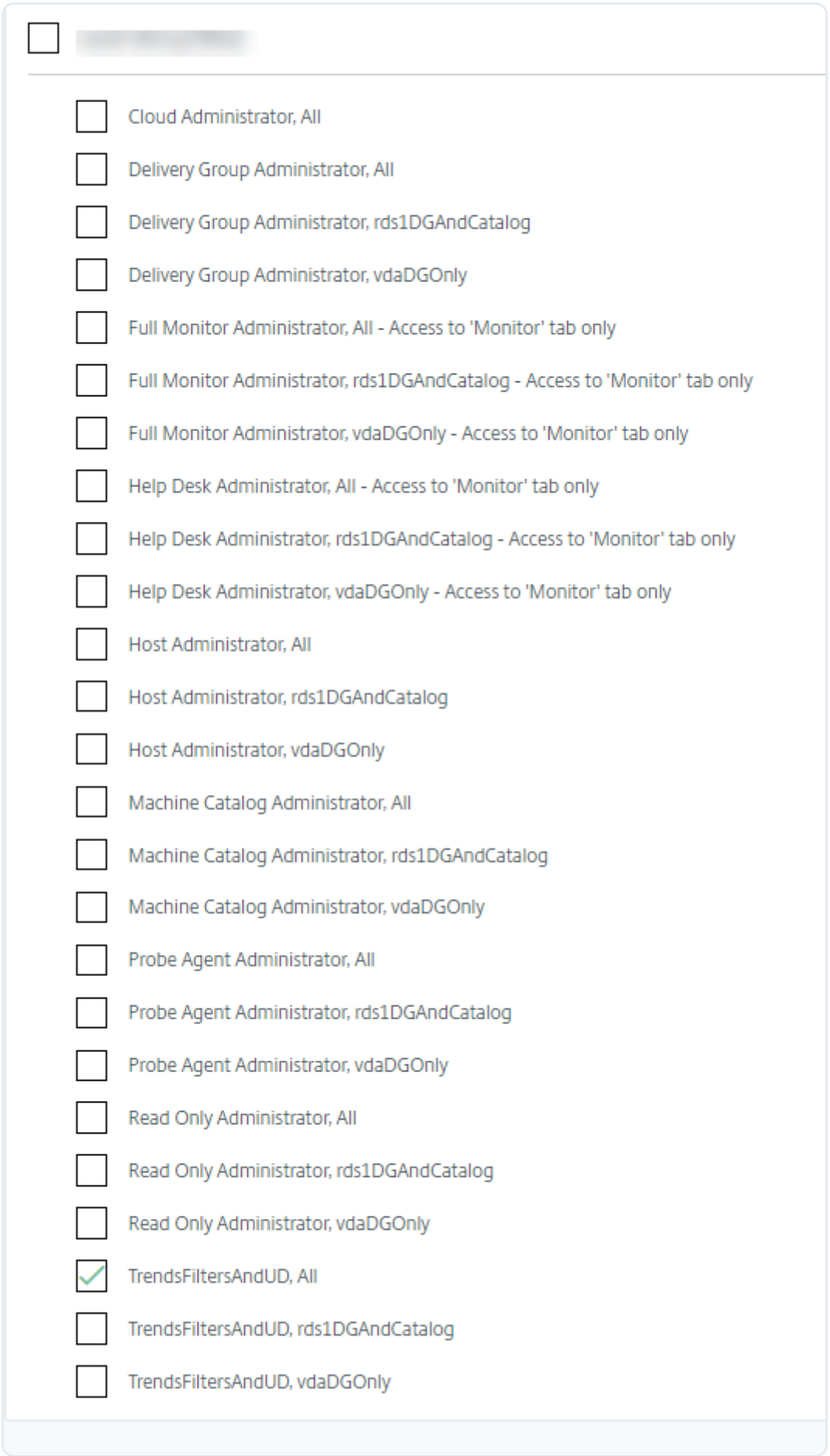
To assign a role (built-in or custom) to a user, from the Citrix Cloud™ menu, go to **Identity and Access Management** > **Administrators**. Here, when you add or edit the access of an administrator, you can select **Custom Access** and one of the listed roles.



You can define custom roles and scopes in **Administrators > Administrators**.

The built-in roles and custom roles are listed for selection with custom scope.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Integrations and data exports

Citrix Monitor now provides a new UI for integrations and data exports. This feature helps to improve the awareness of the various interfaces and third-party integrations available in Citrix Monitor. The newly introduced **Integrations and Data exports** page lists the following:

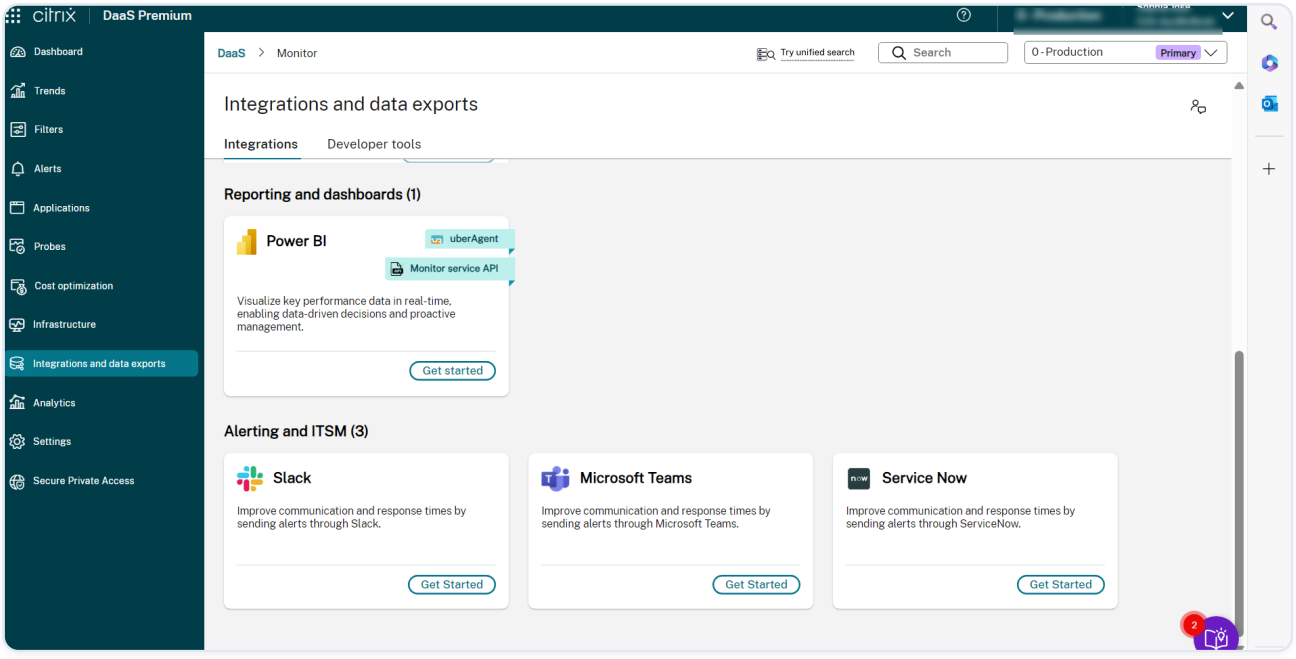
- Available integrations
- Supported developer tools

This page also describes the REST API set up for data exports. Also, provides reference links to the guides and documents to get started with the integrations and developer tools.

The following integration options are provided for collecting Citrix monitoring metrics:

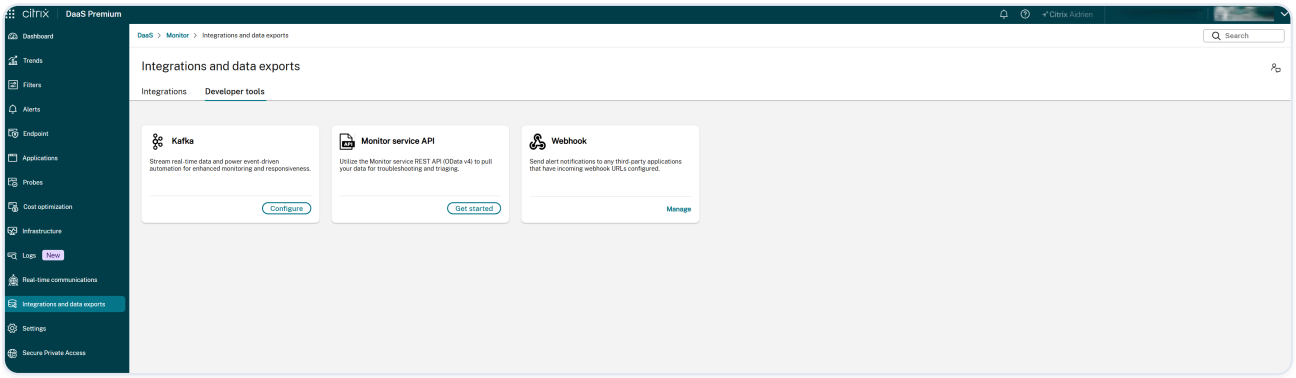
- Citrix Monitor Service API - You can use the Citrix Monitor service API to collect performance data and events from Citrix Monitor and export them to Power BI.
- Alerting and ITSM - You can send alert notifications to the following third-party applications that have incoming webhook URLs configured:
  - Slack
  - Microsoft Teams
  - ServiceNow

Click **Integrations and Data exports** from the left navigation menu. The **Integrations and Data exports** page appears.



Developer tools:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



View available integrations

The **Integrations** tab displays the available integrations for Citrix Monitor. The available integrations are categorized into the following:

- Reporting and dashboards
- Alerting and ITSM

Reporting and dashboards

Power BI can be used for visualizing metrics collected through the Citrix Monitor API. Click **Get started**. The **REST API** developer tools details page appears.

Click Monitor service API to get reference links to resources and blogs with respect to its integration with PowerBI.

This page provides reference links to resources and blogs.

Integrations with alerting and ITSM tools

The alerting and ITSM tools include the following:

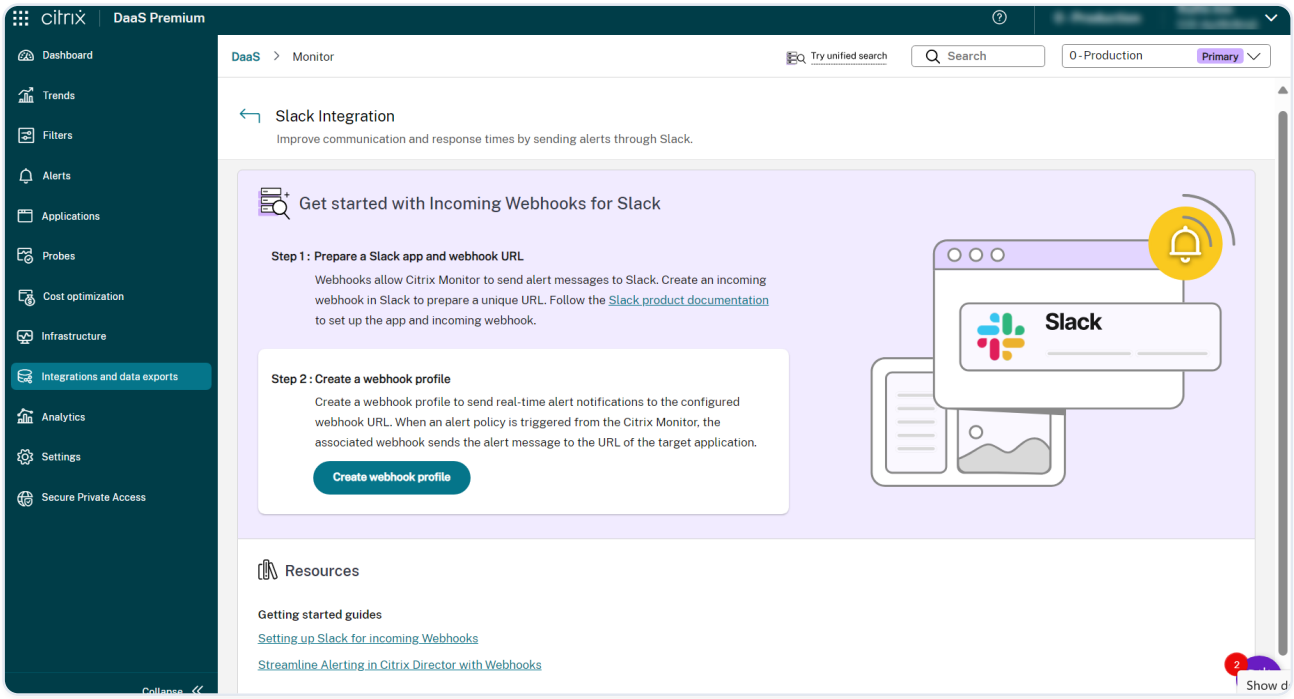
- Slack
- Microsoft Teams
- ServiceNow

To integrate the alerting and ITSM tools with Webhook, click the **Get started** link next to the tools. This link opens the integration page for the specific alerting and ITSM tool, providing details on prerequisites and specific steps to send alerts. You can set up the tools and webhook URL. For example, to integrate Slack, you need to create a channel and Webhook URL following the Slack documentation.

Once that is done, proceed with the second step to create a webhook profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also go through the reference resources. For example, the prerequisites and instructions for integrating with Slack are as follow:



Integration with Webhook

1. Click the **Integrations** tab > **Alerting and ITSM** section > **Get started** next to the selected tool. The **Integration** page for that tool opens up.
2. You can access the reference links to resources and blogs.
3. Follow step 1.
4. Click **Create webhook** profile as part of step 2. The `<name of the tool>` **Create Webhook profile** page appears.
5. Enter the **Name** of the Webhook profile.
6. Enter the **Description** for the Webhook profile.
7. Select the desired **Method** in the **Webhook configuration** section.
8. Enter the **API/Webhook** URL according to the selected method in the previous step.
9. View the **Message** format.
10. Add the key and value in the **Headers** section.
11. Click **Test** to validate the created webhook.
12. If the webhook is validated successfully, click **Create Webhook**. The Webhook is created.
13. View the created webhook profiles at **Developer tools** > **Webhook** > **Manage**. The **Webhook profiles developer tool details** page opens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also create webhook profiles at **Developer tools** > **Webhook** > **Create webhook profiles**.

Integrating the Webhook Profiles with Citrix Alerts

You can view the created webhook profiles at **Alerts** > **Advanced Alert Policies** > **Create Policy** section and use it as part of Citrix Alerts.

To integrate a webhook profile with a new Citrix alert policy, do the following:

1. Click **Alerts** > **Advanced Alert Policies** > **Create Policy**. The **Create advanced alert policy** page appears.
2. Navigate to **Notification channels** > **Use Webhook** section.
3. Select the webhook profile.
4. Save the alert policy.

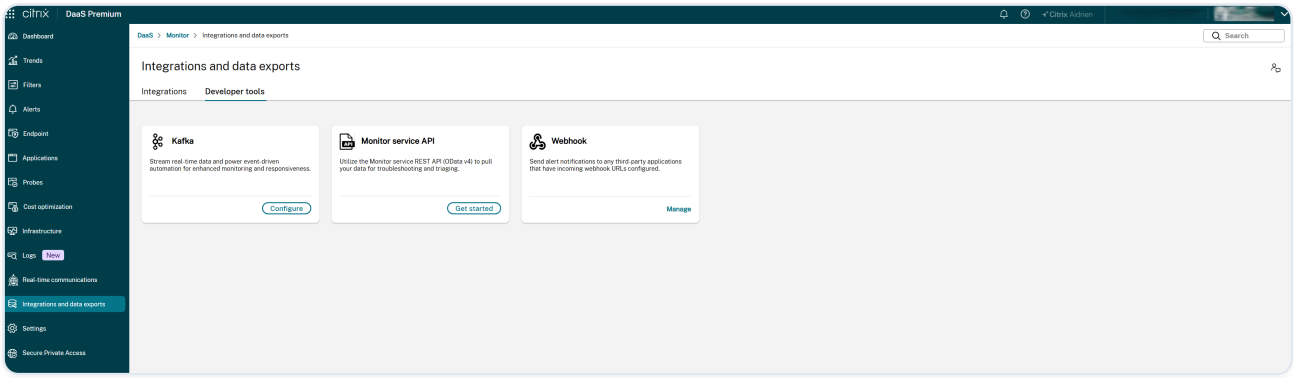
You can integrate a webhook profile with an existing alert policy by doing the following:

1. Click **Alerts** > **Advanced Alert Policies** > **Edit Policy**. The **Edit advanced alert policy** page appears.
2. Navigate to **Notification channels** > **Use Webhook** section.
3. Select or change the webhook profile.
4. Update and save the alert policy.

View supported developer tools

Click **Developer tools** tab to view the available developer tools.

The available developer tools are Monitor service API and Webhook.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

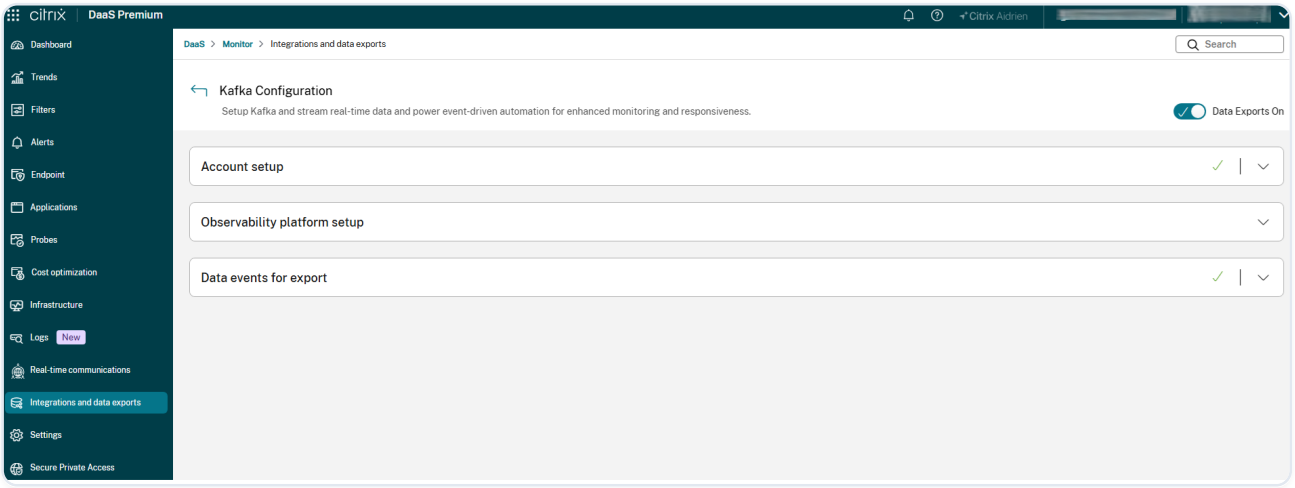
Kafka Data Exports

Kafka Data Exports enables administrators to stream Citrix Monitor event data to external SIEM and observability platforms, such as Splunk, Elastic, and Azure Sentinel. Supported event data includes events from Secure Private Access (SPA) and Device Posture Service (DPS).

To access the configuration, use one of the following paths:

- **Integrations and data exports** > **Developer tools** > **Kafka** on the **Integrations and Data exports** page.
- **Secure Private Access** > **Kafka** in the left navigation menu.

The **Kafka Configuration** page appears.



The **Kafka Configuration** page contains three sections:

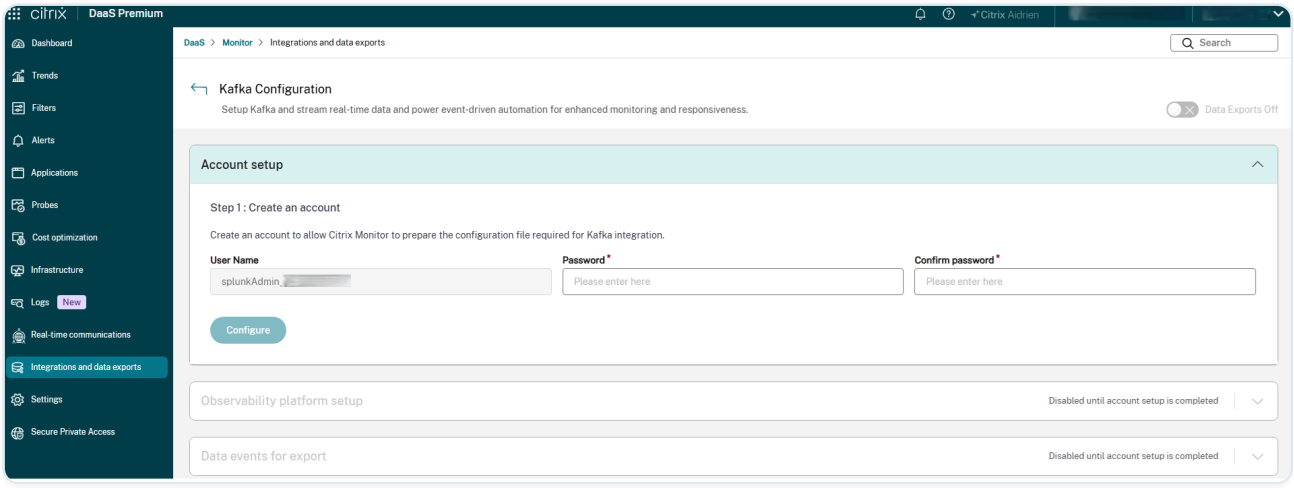
- **Account setup** — Create the Kafka account credentials required for SIEM tool connectivity.
- **Observability platform setup** — Retrieve the connection details needed to configure your chosen observability platform.
- **Data events for export** — Select which event types are streamed to the observability platform.

Use the **Data Exports** toggle in the upper right to enable or disable the export stream at any time.

Account setup

The **Account setup** section lets you create a dedicated account that Citrix Monitor uses to generate the configuration files required for Kafka integration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To set up the account, do the following:

1. Expand the **Account setup** section.
2. In the **Password** field, enter a password for the account. Enter the same password in **Confirm password**.

   NOTE:

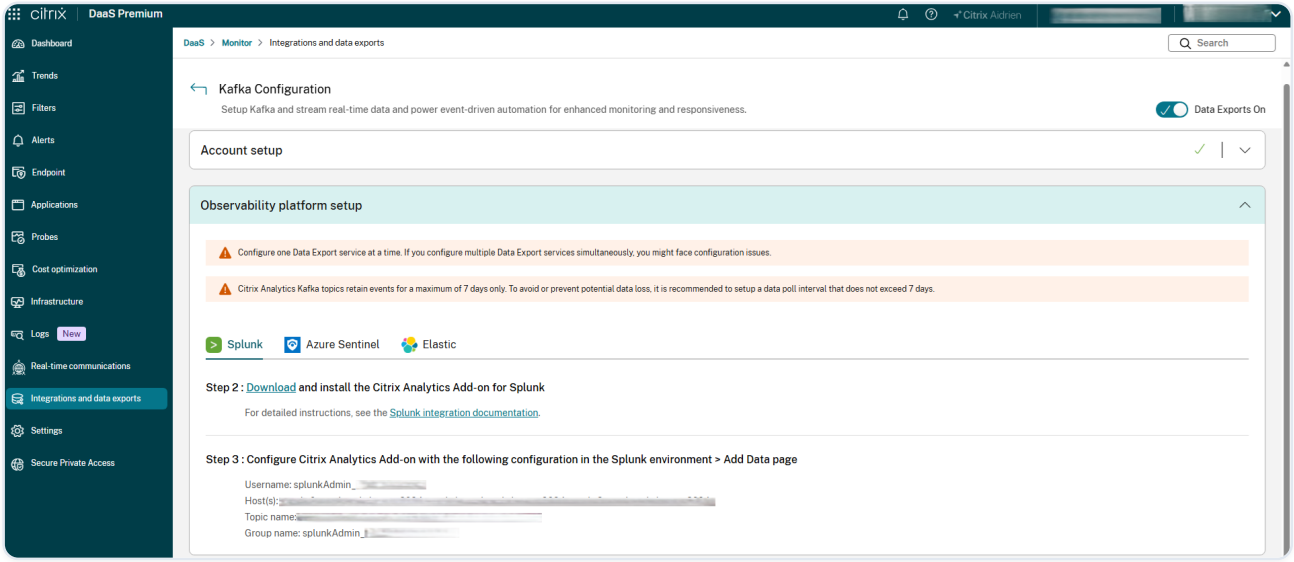
   The **User Name** is generated automatically by Citrix Monitor and cannot be edited.

3. Click **Configure**. Citrix Monitor creates the account and prepares the configuration files.

To update the account password at any time, click **Reset password**, enter a new password, and click **Reset** again.

Observability platform setup

The **Observability platform setup** section provides the Kafka connection details you need to configure your SIEM or observability tool.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following observability platforms are supported:

- **Splunk**
- **Azure Sentinel**
- **Elastic**

To configure your observability platform, do the following:

1. Expand the **Observability platform setup** section.
2. Select the tab for your observability platform (for example, **Splunk**).
3. Follow the on-screen steps:

    - **Step 1:** Complete the **Account setup** section to create the Kafka account credentials. See Account setup.
    - **Step 2:** Download and install the Citrix Analytics Add-on for your platform. For detailed instructions, see the integration documentation linked on the page.
    - **Step 3:** Use the connection details displayed on the page to configure the Add-on in your platform environment. The details include:

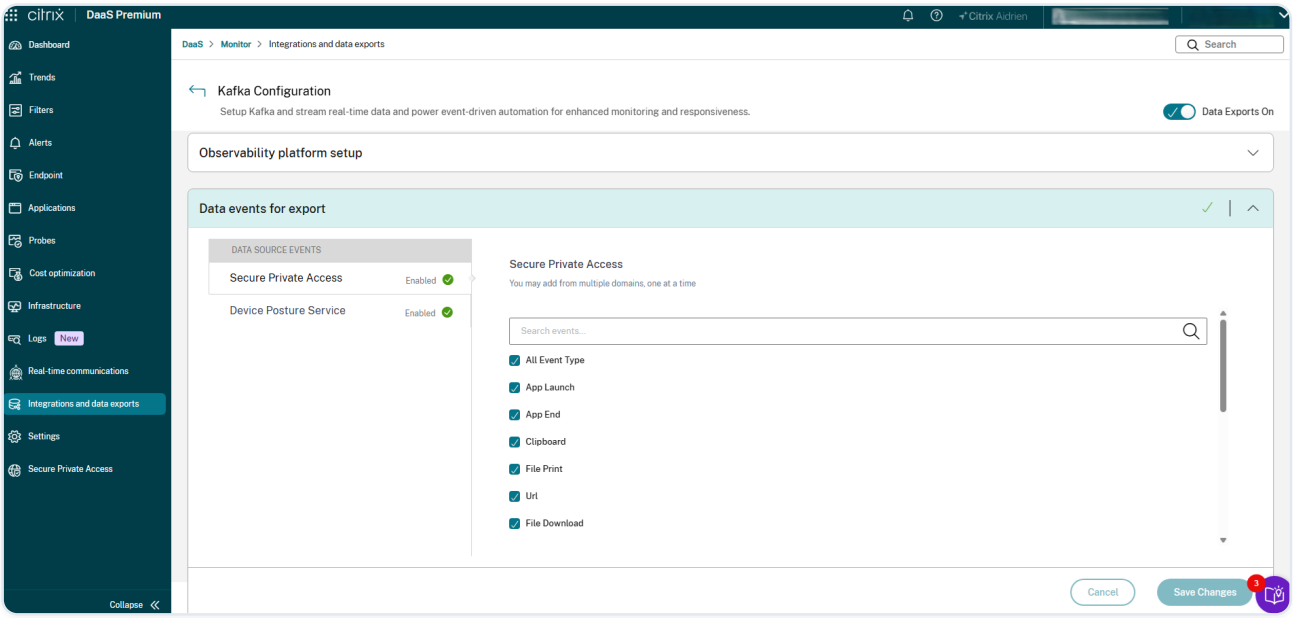
        - **Username**
        - **Host(s)**
        - **Topic name**
        - **Group name**

    For **Azure Sentinel**, see Microsoft Sentinel integration for step-by-step instructions.

Data events for export

The **Data events for export** section lets you choose which event types from each data source are included in the export stream.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The available data sources are:

- **Secure Private Access** — Available to admins with a Secure Private Access entitlement. Supported event types include App Launch, App End, Clipboard, File Print, URL, File Download, and others.
- **Device Posture Service** — Available to all admins. Includes Device Posture Evaluation events.

To configure event types for export, do the following:

1. Expand the **Data events for export** section.
2. In the **Data Source Events** panel, select a data source (for example, **Secure Private Access**).
3. In the right panel, select the event types to include in the export. Use the search field to filter events by name. Select **All Event Type** to include all available events for that source.
4. Repeat for each data source as needed.
5. Click **Save Changes**.

Monitor service API

Click **Get started**. The **Monitor Service API** developer tool details page opens. You can access the reference links to resources and blogs.

Webhook

You can view and create webhook profiles at **Developer tools** > **Webhook** > **Create webhook profiles**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Sentinel integration

Kafka Data Exports in Citrix® Monitor can stream **Secure Private Access (SPA)** and **Device Posture Service (DPS)** events into Microsoft Sentinel through Logstash. The **Citrix SPA Sentinel App** in the Microsoft Sentinel Content hub supplies the data connector and the connection information Logstash needs to forward the events.

To integrate with Microsoft Sentinel, install the Citrix SPA Sentinel App solution from the Content hub and configure Logstash, as described in the following sections.

Prerequisites

- A Microsoft Sentinel workspace and permission to install a solution from the Content hub.
- A Logstash host running a Logstash version supported by the Microsoft Sentinel output plugin. For the supported versions, see Logstash plugin prerequisites.
- Ensure that the Kafka Data Exports broker endpoints for your region are in the allow list in your network:

ENDPOINT	UNITED STATES REGION	EUROPEAN UNION REGION	ASIA PACIFIC SOUTH REGION
Kafka brokers	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

To validate network connectivity to a Kafka broker, run the following commands in your environment and confirm that they succeed. Replace the endpoint with a broker for your region.

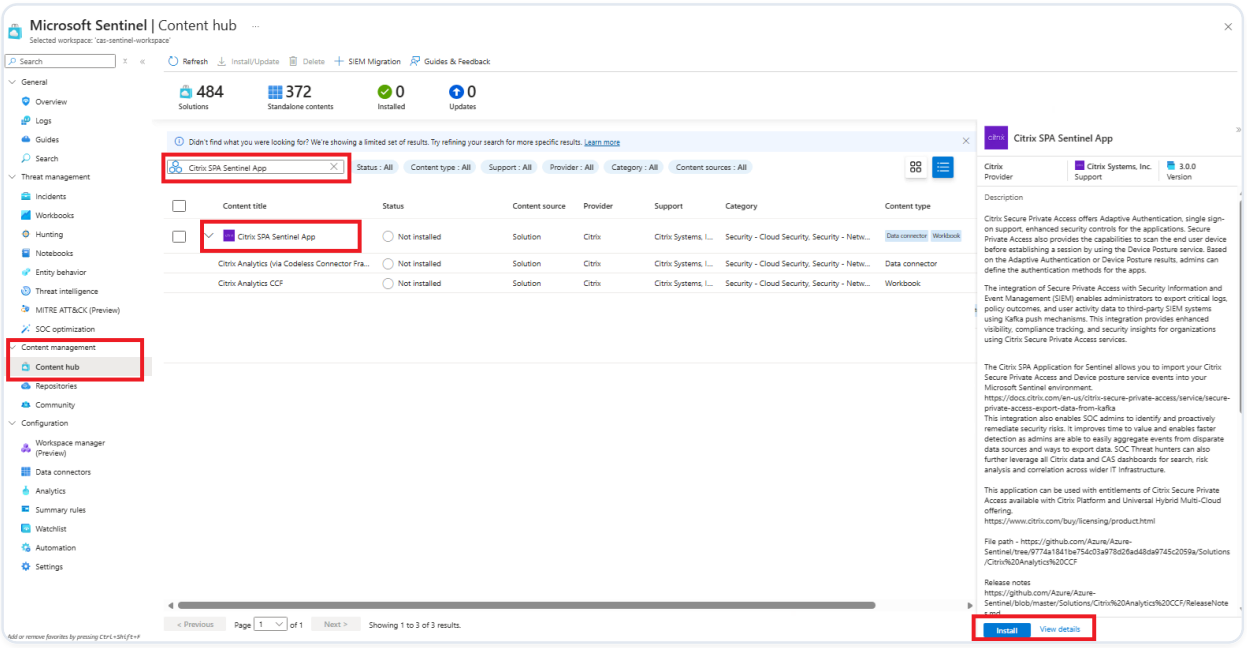
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
telnet casnb-0.citrix.com 9094

openssl s_client -tls1_3 -connect casnb-0.citrix.com:9094 -showcerts
< /dev/null
```

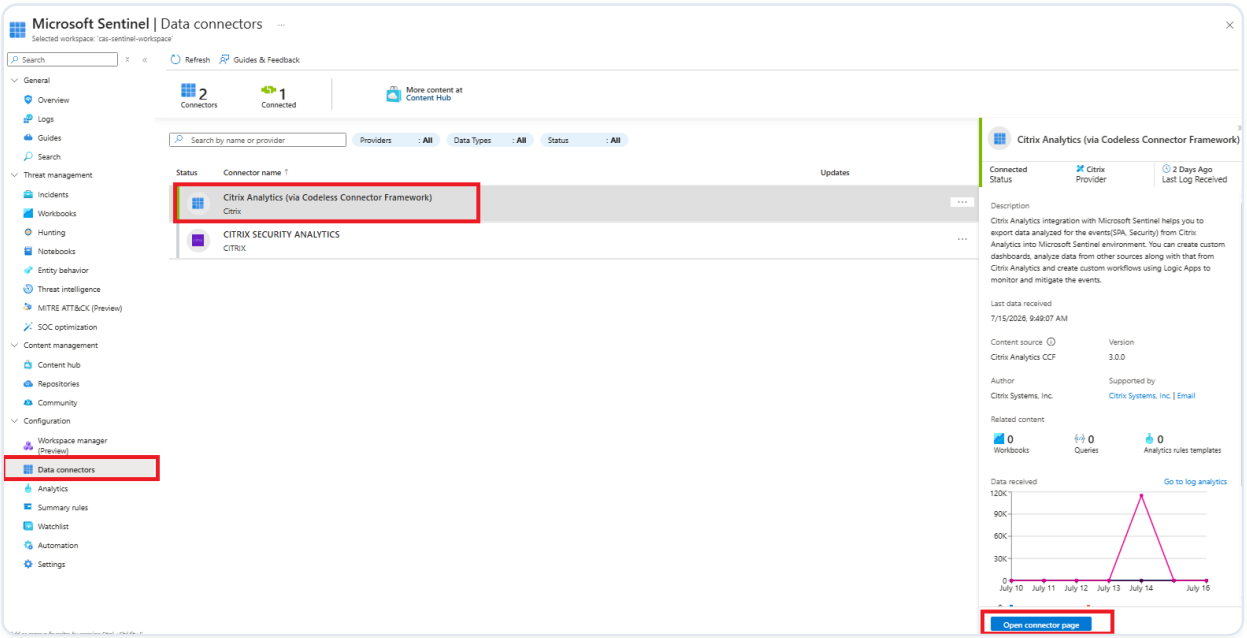
Install the Citrix SPA Sentinel App

1. In the Azure portal, open **Microsoft Sentinel** and select your workspace.
2. Under **Content management**, click **Content hub**.
3. Search for **Citrix SPA Sentinel App** and click **Install**.

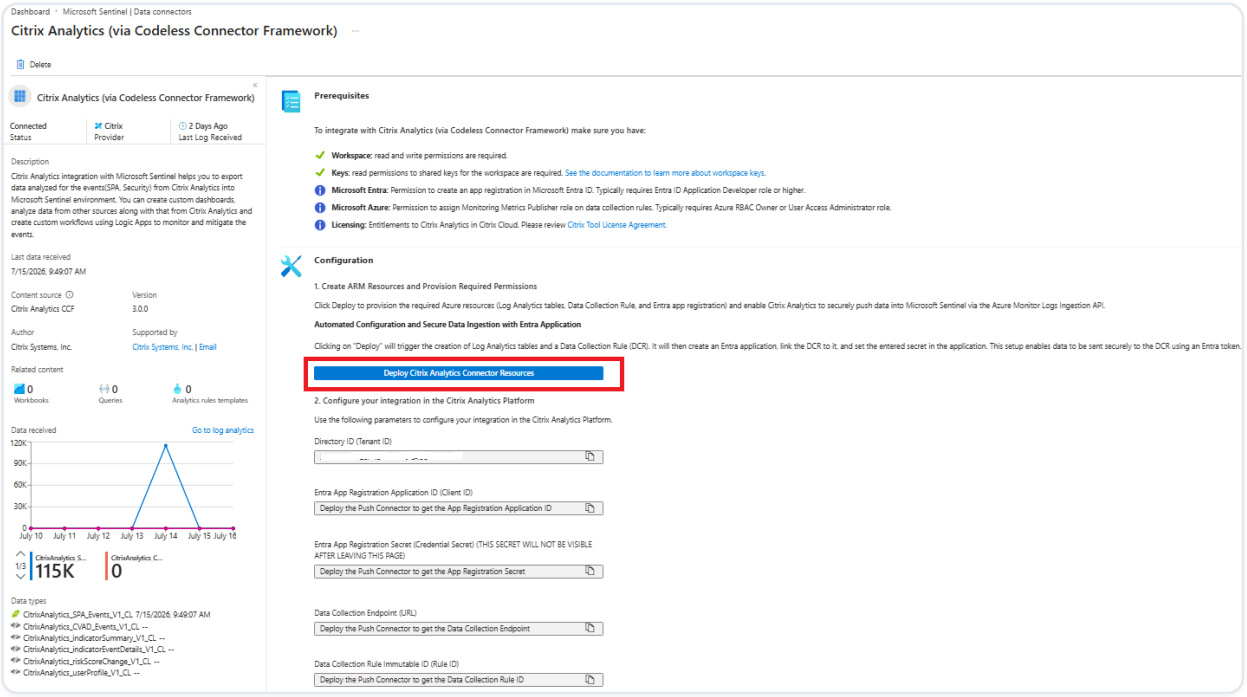


4. Go to **Configuration** > **Data connectors** and open the data connector shipped with the solution. Click **Open connector page**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Deploy the connector resources, including the data collection rule (DCR) and the Microsoft Entra application used for authentication. When the deployment finishes, keep the **connection information** shown on the data connector page open — you paste it into the Logstash configuration in the next step.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For security reasons, the **Entra App Registration Secret** is shown only once. It is no longer visible after you leave or refresh the data connector page. While the resources are deploying, copy and save the secret as soon as it appears. If the **Entra App Registration Secret** disappears before you copy it, click **Revoke access** to delete the Entra application and remove the data connector, and then deploy the connector resources again to generate a new secret.

Configure Logstash

1. In Citrix Monitor, open **Integrations and data exports** > **Developer tools** > **Kafka** to display the **Kafka Configuration** page, then create the account and download the configuration files:
   a. Complete the **Account setup** section to create the Kafka account credentials. For the detailed steps, see Account setup.
   b. Expand the **Observability platform setup** section and select the **Azure Sentinel** tab.
   c. Download the Logstash configuration file and JKS truststore generated for your account.
2. On the Logstash host, install Logstash and the Microsoft Sentinel output plugin.
3. On the host machine where you have installed Logstash, place the downloaded files in the specified directory:

HOST MACHINE TYPE	FILE NAME	DIRECTORY PATH
Linux	DIRECTOR_AzureSentinel_LogStash_Config.conf	For Debian and RPM packages: `/etc/logstash/conf.d/`
		For .zip and .tar.gz archives: `{extract.path}/config`
	kafka.client.truststore.jks	For Debian and RPM packages: `/etc/logstash/ssl/`
		For .zip and .tar.gz archives: `{extract.path}/ssl`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HOST MACHINE TYPE	FILE NAME	DIRECTORY PATH
Windows	DIRECTOR_AzureSentinel_LogStash_Config.conf	`C:\logstash-x.xx.x\config`
	kafka.client.truststore.jks	

4. Open the Logstash configuration file and do the following:

   a. In the input section of the file, enter the following:

   - **Password**: The password of the account that you created during Account setup in Citrix Monitor (**Integrations and data exports** > **Developer tools** > **Kafka**).
   - **SSL truststore location**: The location of your SSL client certificate. This is the location of the kafka.client.truststore.jks file on your host machine.

```
input {
  kafka {
    bootstrap_servers => "casnb-0.citrix.com:9094,casnb-1.citrix.com:9094,casnb-2.citrix.com:9094,casnb-3.citrix.com:9094"
    topics => ["cas.siem.aec719c5-035e-40bb-87f9-310dd1f1de29"]
    group_id => "splunkAdmin_ab2wib4x8s6a-group"
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='splunkAdmin_ab2wib4x8s6a' password='<your password>';"
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
}
```

   b. In the **output (Microsoft Sentinel)** section, paste the connection information from step 5 of Install the Citrix SPA Sentinel App — the data collection endpoint (DCE), the data collection rule (DCR) immutable ID, and the Entra application credentials (tenant ID, client ID, and the Entra App Registration Secret).

```
output {
  if [event_type] in ["datasourceSPAEventDetails", "datasourceDPSEventDetails"] {
    microsoft-sentinel-log-analytics-logstash-output-plugin {
        client_app_Id => "<application id>"
        client_app_secret => "<application secret>"
        tenant_id => "<tenant id>"
        data_collection_endpoint => "<data collection endpoint>"
        dcr_immutable_id => "<data collection rule id>"
        dcr_stream_name => "Custom-CitrixAnalytics_SPA_Events_V1"
    }
  }
}
```

5. Restart Logstash to apply the configuration.

Select SPA and DPS event types

Choose the event types that Kafka Data Exports streams to Sentinel from **Data events for export** on the Kafka Data Exports page:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Secure Private Access** — App Launch, App End, Clipboard, File Print, URL, File Download, and related event types.
- **Device Posture Service** — Device Posture Evaluation events.

For background on the upstream Kafka export, see Export data from Kafka for Secure Private Access.

Verify data ingestion

After Logstash starts forwarding, events appear in your Microsoft Sentinel workspace within a few minutes. Check the **Data received** indicator on the data connector page to confirm that ingestion has started.

To confirm that events are landing in the table, open **Microsoft Sentinel** > **Logs** and run the following query:

```
CitrixAnalytics_SPA_Events_V1_CL

| where TimeGenerated > ago(24h)

| summarize count() by event_type, event_category

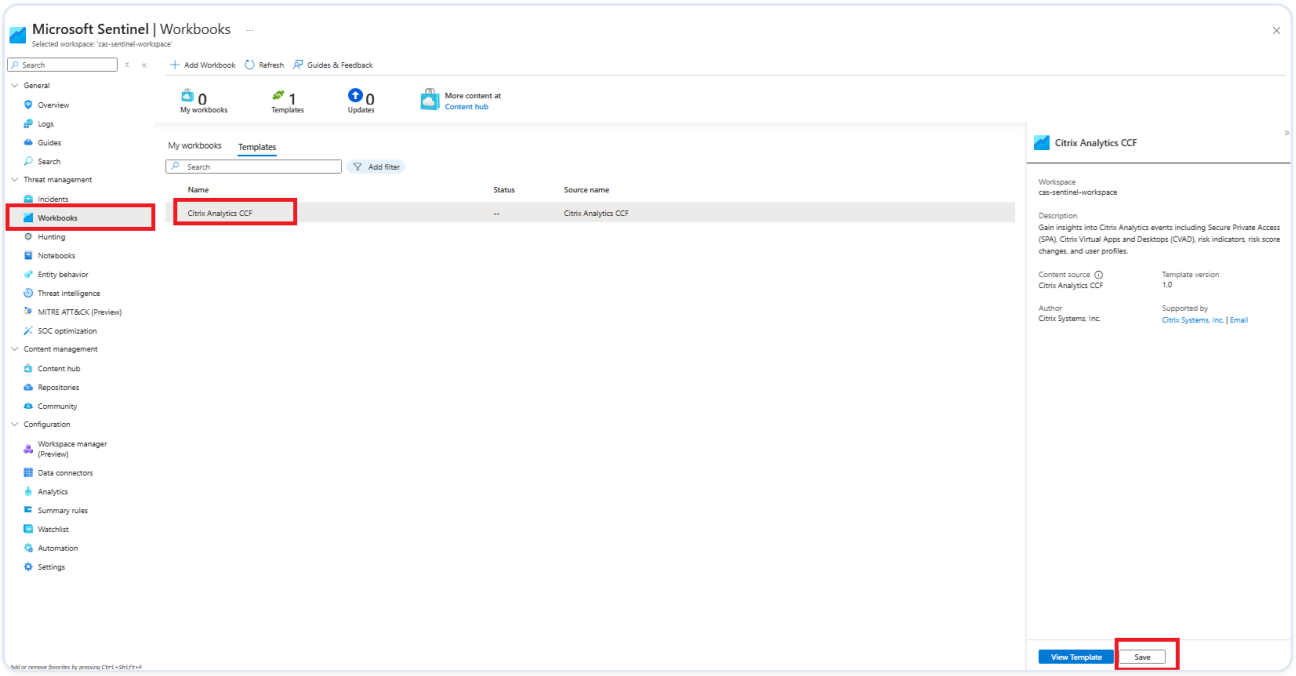
| order by count_ desc
```

The query returns the event count for the last 24 hours, grouped by event type and category. If it returns results, data is being ingested successfully.

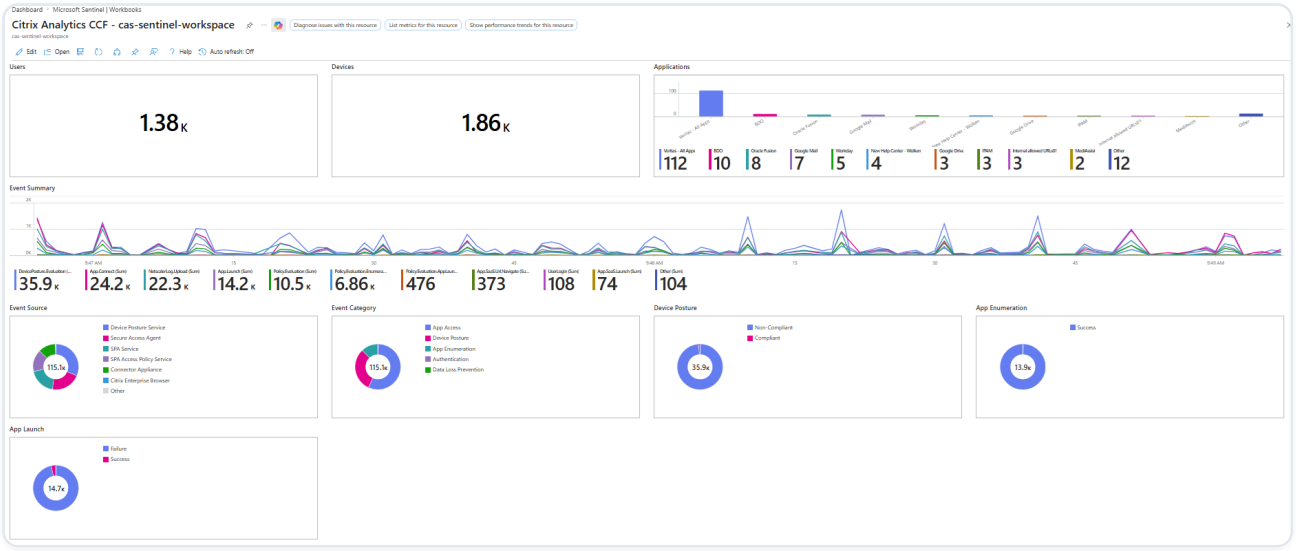
View workbook

The Citrix SPA Sentinel App ships a workbook template. To use it, open **Microsoft Sentinel** > **Threat management** > **Workbooks** > **Templates**, select **Citrix Analytics CCF** workbook, and click **Save**. Then, select **View saved workbook** to open it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The workbook provides a **Secure Private Access** tab that visualizes SPA and DPS activity.



The workbook template is a starting point. Because all events are stored in the `CitrixAnalytics_SPA_Events_V1_CL` table, you can also create your own visualizations tailored to your needs — write custom Kusto queries and build workbooks or dashboards that highlight the metrics and insights most relevant to your organization.

Secure Private Access

Citrix Monitor allows help desk admin or full admin to monitor and troubleshoot all Secure Private Access sessions.

To begin montioring Secure Private Access sessions in your site, see to the following:

- Secure Private Acess tab

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Monitor and troubleshoot Secure Private Access
- Secure Private Access alerts

Secure Private Access tab on Monitor

The **Secure Private Access** tab on Monitor provides a dedicated place for all new features related to Secure Private Access. This tab offers details on the supported functions for Secure Private Access, giving administrators a central location to access and manage these features.

Key benefits

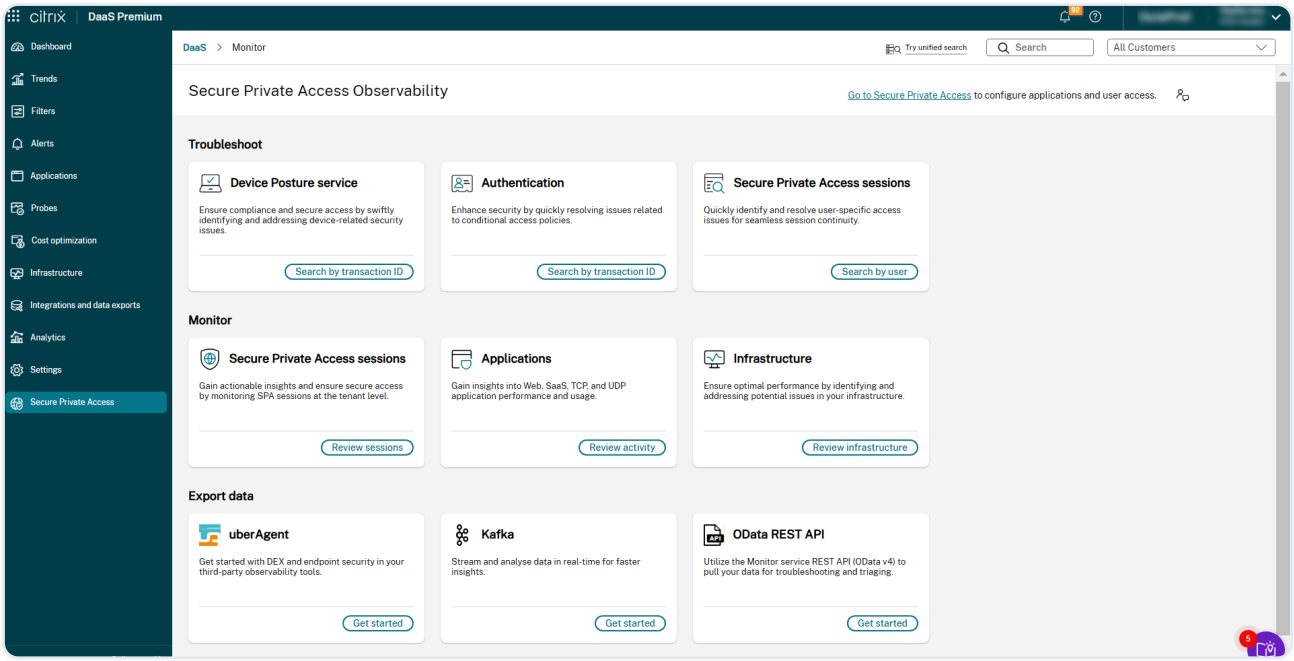
- Centralized information: Administrators can easily see all supported troubleshooting features for Secure Private Access in one place.
- Enhanced observability: The new left navigation bar in the Monitor UI lists all Secure Private Access services, including Secure Private Access sessions, applications, and device posture, providing better observability.
- Improved navigation: The Secure Private Access tab includes hyperlinks to different pages, making it easier for administrators to navigate to various features and functions.

Requirements

- The **Secure Private Access** tab is visible to all customer admins.
- Secure Private Access-specific cards (Secure Private Access sessions and applications) are clickable only when the customer has Secure Private Access entitlement and the admin has Secure Private Access full admin or read-only admin permissions.

To view the **Secure Private Access** page, click the **Secure Private Access** tab from the Monitor UI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Visibility for Secure Private Access Service

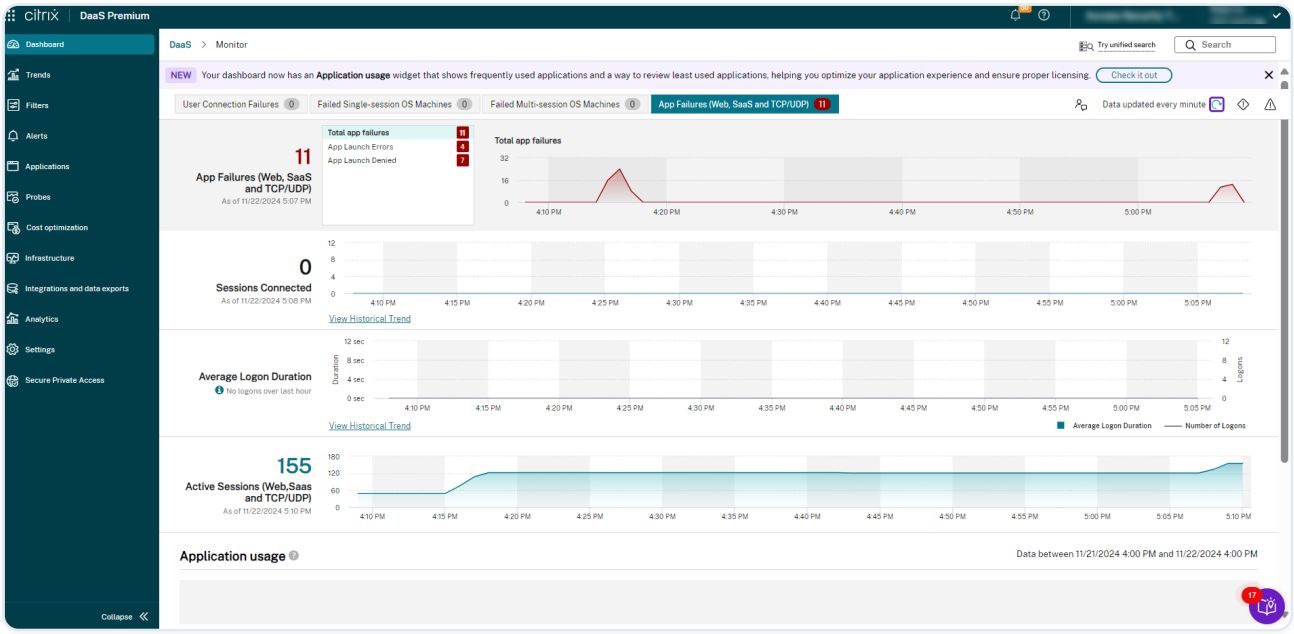
To provide detailed monitoring and visibility for Secure Private Access applications and users, Monitor is now enhanced to include Secure Private Access session visibility. The **Filters** tab and **Dashboard** provide detailed Secure Private Access session information.

Key features

- **Filter Secure Private Access Sessions**: You can now filter Secure Private Access sessions in the **Filters** > **Sessions (Web, SaaS, and TCP/UDP)** tab.
- **Filter Secure Private Access Applications**: You can also filter Secure Private Access applications in the **Filters** > **Applications (Web, SaaS, and TCP/UDP)** tab.
- **App Failures and Active Sessions**: Monitor app failures for web/SaaS and TCP/UDP apps, and view active sessions for web/SaaS apps in the Dashboard.

Dashboard:

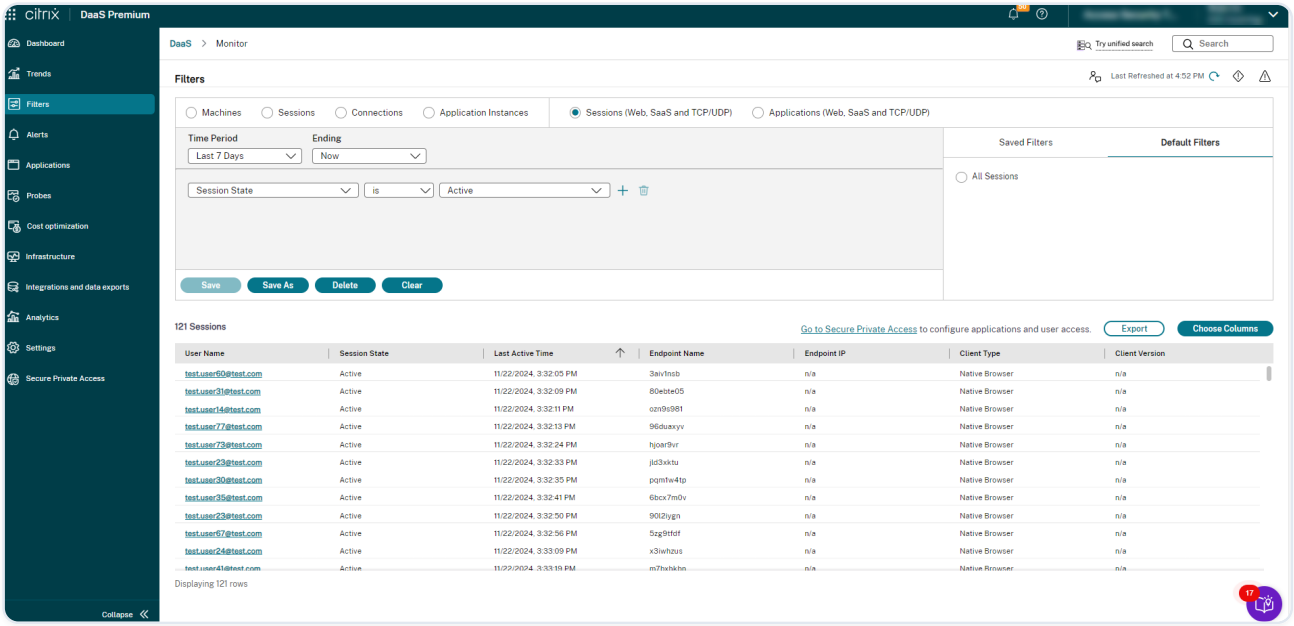
© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

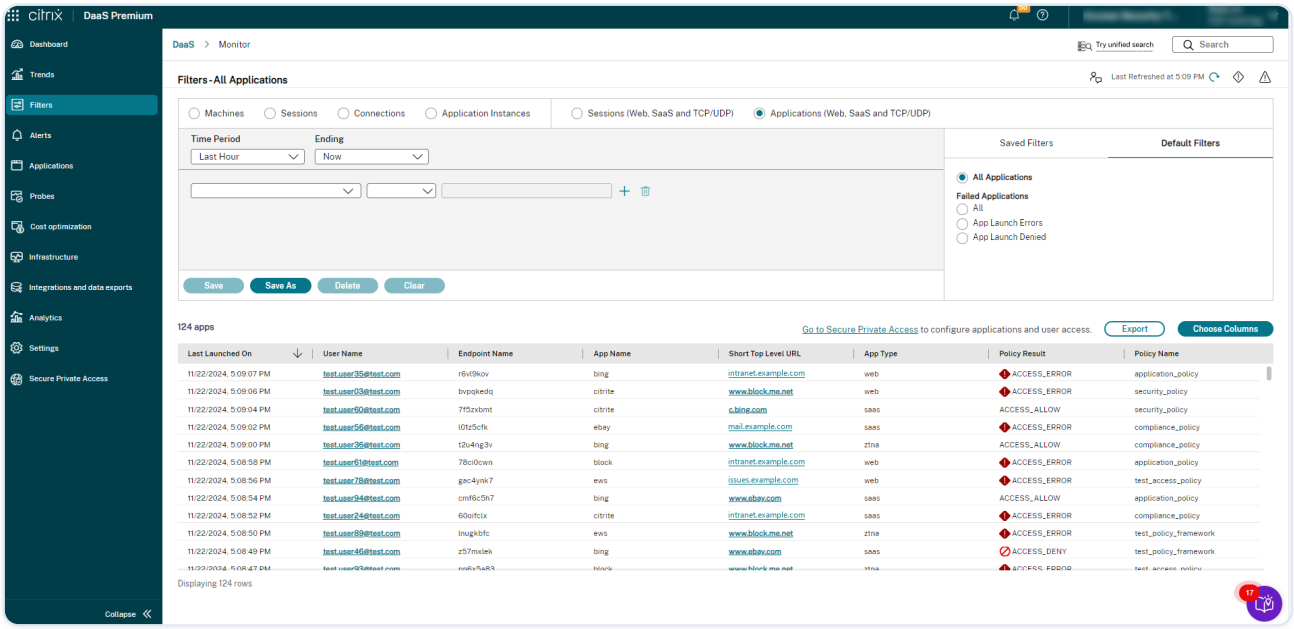
- The number displayed in the dashboard next to App Failures (Web, SaaS, and TCP/UDP) represents the number of application failures in the last hour.
- The number displayed in the dashboard next to Active Sessions (Web, SaaS, and TCP/UDP) represents the current number of active Secure Private Access sessions in the last hour.

Filter all Secure Private Access Sessions:



Filter all Secure Private Access Applications:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Monitor and troubleshoot Secure Private Access

Secure Private Access is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor, in addition to the Secure Private Access dashboard.

Service entitlements

To use the DaaS Monitor feature with Secure Private Access, you must have both Secure Private Access and DaaS entitlements.

Supported clients

- Citrix Workspace™ app - 2409 and later
- Citrix Secure Access for Windows - 24.8.1.19 and later
- Citrix Secure Access for macOS - 24.10.1 and later

How to access Monitor

You can access Monitor from the Secure Private Access dashboard (**Go to Monitor**) or from the Citrix DaaS™ service tile.

Session definitions

A Secure Private Access session offers a comprehensive summary of an end-user's session lifecycle, application activity, and user experience on a specific device. A session serves as a unified record for troubleshooting and analysis by providing visibility into the following aspects:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Detailed insights into how applications are accessed, including launch hops, network topology, connections, and routing details. These details are crucial for resolving issues related to access policies.
- Tracks all session activity from:
  - Browsers accessing web or SaaS applications.
  - The Citrix Secure Access client for private applications using TCP/UDP protocols.

Some of the key characteristics of a Secure Private Access session are:

- Each session is assigned a unique ID for tracking and analysis.
- A single session can include multiple app launches and provides a comprehensive view of the user activity within that specific session.
- For each app, the session tracks:
  - The security controls that apply to the app.
  - The policy display name and ID that triggered the security controls.
  - The condition that resulted in the policy being enforced.
- The session tracks all the internal domains that a user has visited in Citrix Enterprise Browser™ providing insights into the user navigation within the secure environment.

Web/SaaS app sessions

The session starts and ends for Web/SaaS apps is defined as follows:

- Start: Citrix Enterprise Browser or Chrome Enterprise Premium is opened in the Citrix Workspace app and applications are accessed.
- End: A session ends in the following scenarios.
  - You close the Citrix Enterprise Browser.
  - After 30 minutes of inactivity and no session activity is reported.

    The Citrix Enterprise Browser/Chrome Enterprise Premium client sends a session activity every 15 minutes to Monitor. If this session activity is not received for 30 minutes, which might occur due to the following reasons:
    - Network failure.
    - Internet connectivity issues.
    - Session closure after the 360-minute interval without session activity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For apps launched through native browsers (agentless), the session ends after 120 minutes of inactivity.

TCP/UDP app sessions

The session starts and ends for TCP/UDP apps is defined as follows:

- Start: You log in to the Citrix Secure Access™ client and access the apps.
- End: A session ends in the following scenarios.
  - You log out of the Citrix Secure Access client.
  - After 30 minutes of inactivity and no session activity is reported.

Agentless app sessions

The session starts and ends for the agentless apps is defined as follows:

- Start: You launch the app from Citrix Workspace app or from a web browser.
- End: A session ends after 120 minutes of inactivity.

KNOWN LIMITATION:

The agentless app sessions are terminated after 120 minutes of inactivity regardless of the timeout settings configured in the Secure Private Access console (**Settings > Timeouts**).

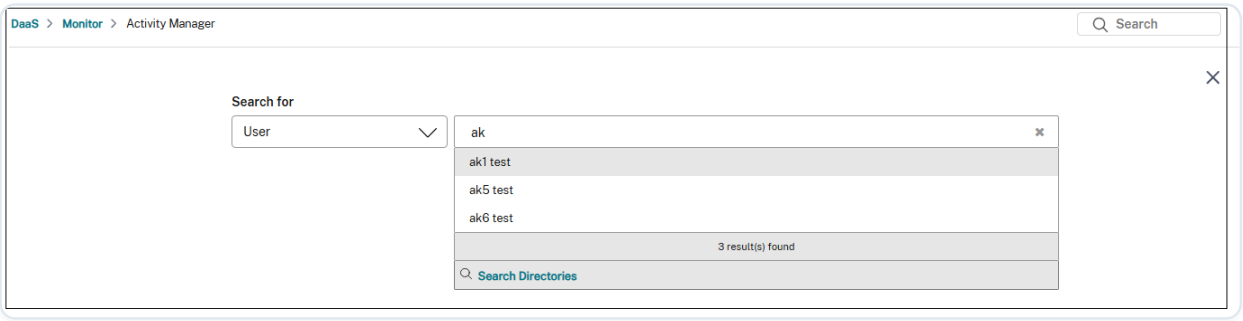
View a Secure Private Access session by user

View a session using the Search field

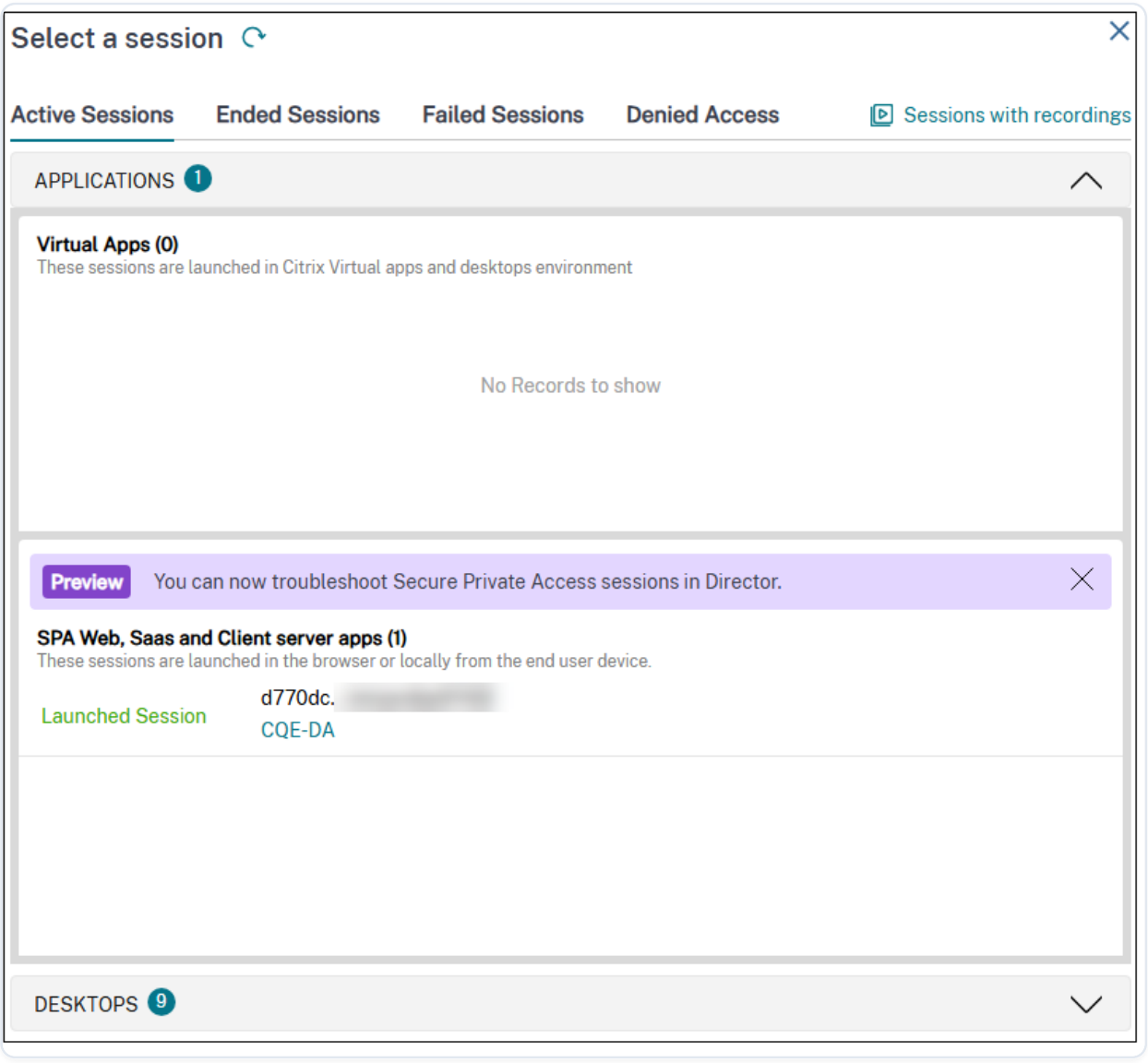
1. On the Monitor dashboard, click **Search** and enter the user name. The **Select a session** screen appears.

   . If you don't find the entered user name, click **Search Directories** to find the user name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



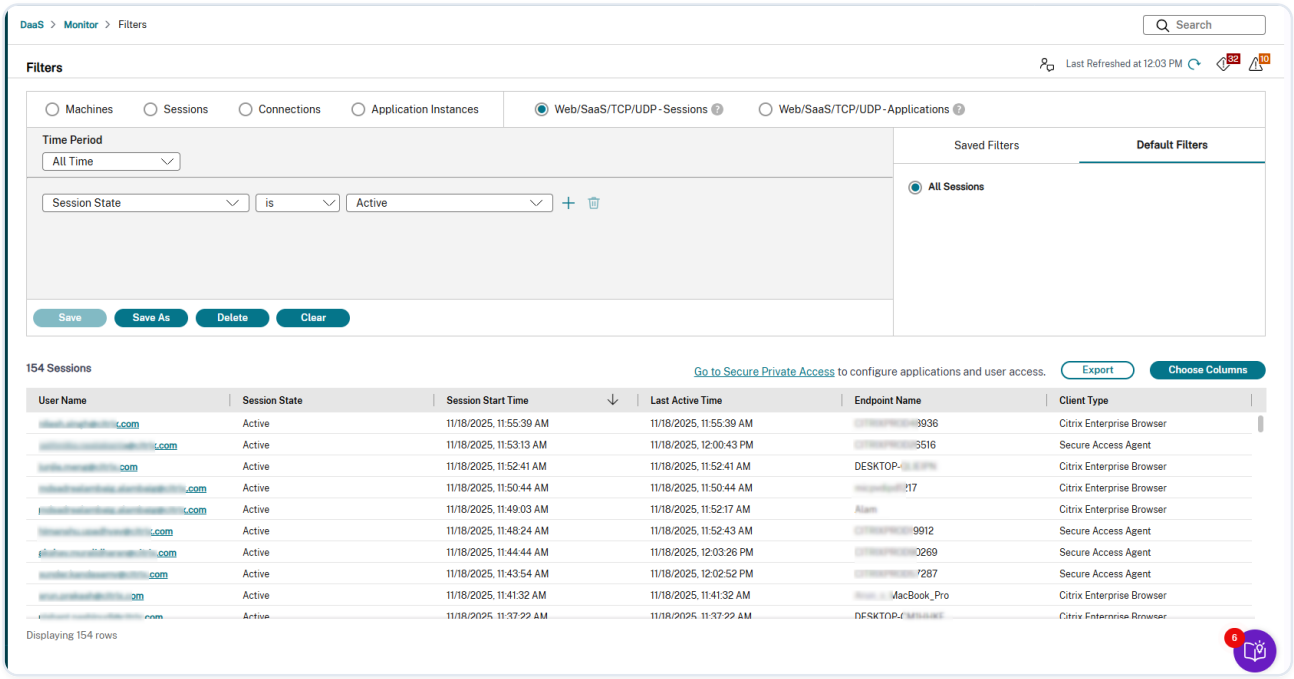
2. Select the required user. The **Select a session** screen appears.



View a session from the Filters page

You can search for the sessions from the **Filters** page wherein you can search for the specific sessions using the various conditions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Perform the following steps to view a user session from the **Filters** page:

- Refine your search based on the various filters such as the machines, sessions, connections, Application instances, Secure Private Access sessions, and Secure Private Access applications. You can also refine your search based on the timeline.
- Use the drop-down lists to select further filter criteria (for example **Associated user**, **Endpoint IP** and so on). For more information, see Filter data to troubleshoot failures.

The list of sessions associated with the specified user is displayed.

Activity Manager for Secure Private Access session

Citrix Monitor offers the Activity Manager view for Secure Private Access sessions, which gives you an overall view of the session activities. The Activity Manager provides a comprehensive view of all apps and desktops that are successfully opened, failed to open, and the outcome of the policies set in the Secure Private Access app.

The Activity Manager contains the following tabs:

Available Apps: Displays the apps that are available in the Citrix Workspace app. This section shows the last enumeration attempt of the apps and the status of the enumeration attempt.

Launched Apps: Displays the apps that are opened in the Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If an application is accessed multiple times in the same session, only the details of the most recent access are captured.

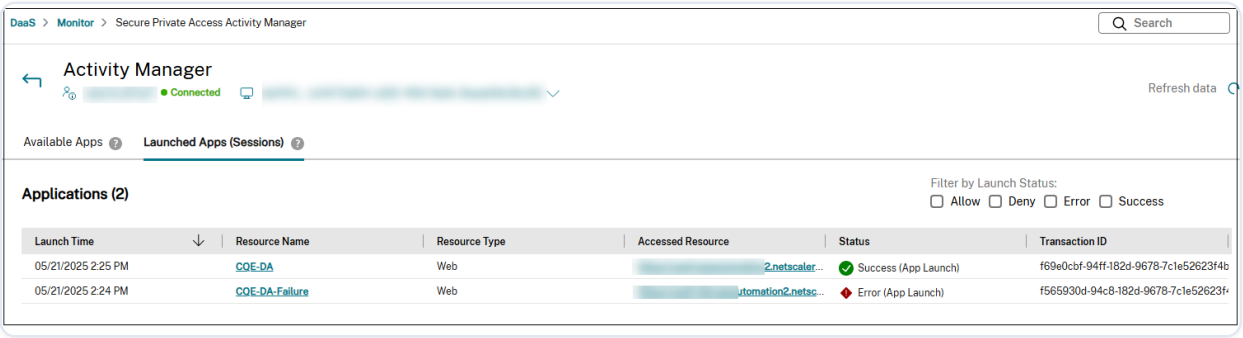
View Activity Manager

To view the Activity Manager, do the following:

1. On the Monitor dashboard, click **Search** and enter the user name.

   . If you don't find the entered user name, click **Search Directories** to find the user name.

2. Select the required user. The **Select a session** screen appears.
3. Select an active session that is opened using the Secure Private Access session. The Activity Manager for the selected session appears.



4. Click **Available Apps** to view apps that are available in the Citrix Workspace app or click **Launched Apps (sessions)** to view the apps that are opened in the Citrix Workspace app.

   You can categorize and filter resources based on their access status for users. These statuses reflect the outcome of the policies configured within the Secure Private Access app.

   - **Allow:** Indicates that the Secure Private Access policy allows access to the specified resource. As a result, the resource is visible and accessible within the user's Citrix Workspace app.
   - **Deny:** Indicates that the Secure Private Access policy prevents the user access to the resource. Although the resource might be visible within the user's Citrix Workspace application, it remains inaccessible, indicating access restrictions resulting from policy enforcement.
   - **Error:** Indicates a scenario where a user is intended to have access to a resource according to the Secure Private Access app policies. However, due to an underlying issue,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the resource is not functioning correctly or is unavailable within the Citrix Workspace app. The error might be related to enumeration or session.

- **Success:** Indicates whether the app launch was successful.

Secure Private Access Session Details page

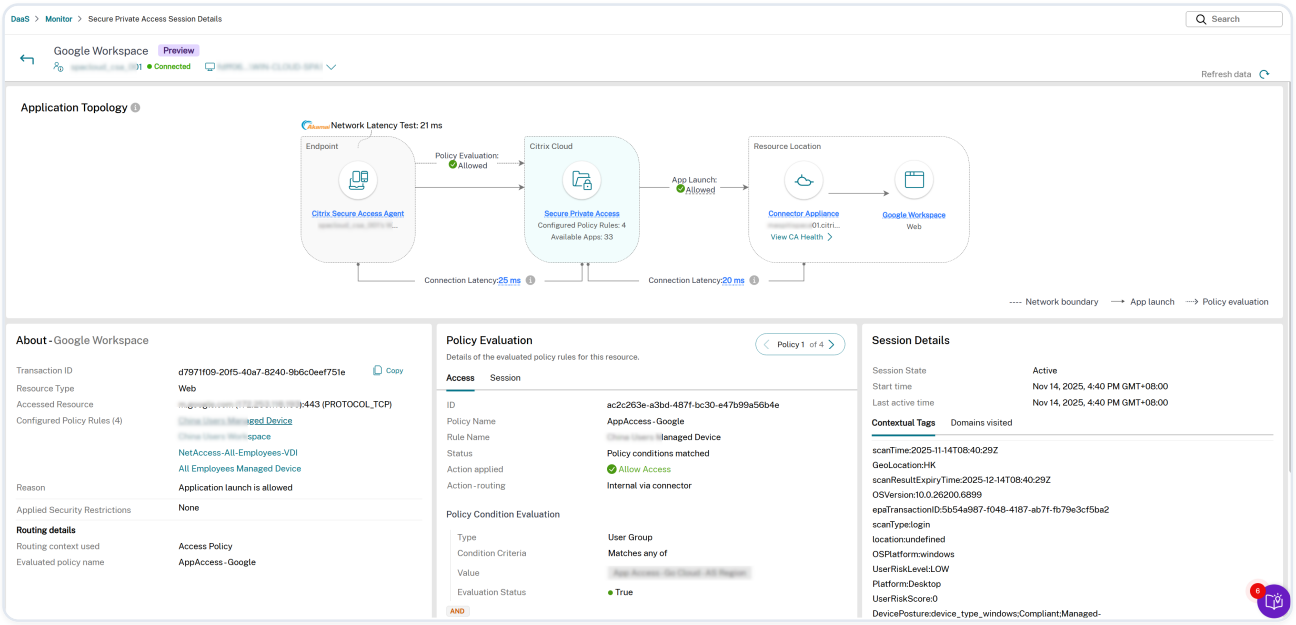
A Secure Private Access Session Details page contains the following four panes:

- **Application topology:** Provides the flow of the app launch process. Also, provides complete details about the app. The endpoint connects to the Citrix Gateway and Citrix Gateway connects to the Secure Private Access plug-in. Using the information from the Secure Private Access plug-in, the app is launched.

  You can view the application topology of an app from the **Available apps** or **Launched apps** section of the Activity Manager. You can also view the application topology for the apps for which access is denied from the **Denied Access** tab.
- **Endpoint details:** Displays key information about the client device and network used to access the application. Hover over Endpoint to view detailed information.
- **About:** Displays additional information regarding the Web/SaaS, TCP/UDP and agentless apps for both the successfully launched apps and the failed apps.
- **Policy Evaluation:** Displays information related to the policy, such as rules, actions, and conditions in the **Access** and **Session** tabs.
  - The access policy details can be viewed under the **Access** tab.
  - The session policy details can be viewed in the **Session** tab.
- **Session Details:** Displays session details for a successfully established session. For a failed session, the reason for session failure is displayed.
- **Hop by hop latency:** Displays the latency details for each hop in the application topology, including the Connector Appliance to backend application hop. Helps admins triage and isolate performance or slowness issues across the multiple hops.

The following figure displays a sample Secure Private Access Session Details page for a successful app launch.

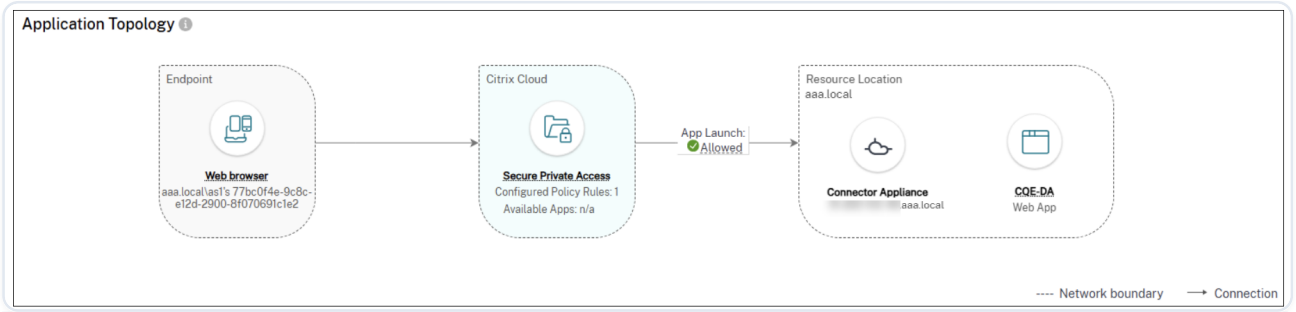
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Application topology

In a successful application launch scenario, the Application Topology represents the entire communication flow in a uniform color. Conversely, when an application launch fails due to issues such as a non-reachable Connector Appliance or an unavailable backend server, Application Topology displays the specific segment of the flow where the failure occurs in a different color. For example, if the Connector Appliance is unreachable, the connection between Citrix Cloud™ and Resource Location might be highlighted in red indicating the failure. For Chrome Enterprise Premium sessions, the topology also reflects the application route (`internal`, `external`, or `external_fixed_ip`) used for the launched app. For the mapping between these terms and the **Action routing** field on the Session Details page, see Application route vocabulary.

The following figures display a sample application flow.



FIELD NAME	DESCRIPTION
Endpoint	Displays the endpoint where the app is opened. The possible options are Citrix Workspace app and Citrix Secure Agent. The device ID is displayed. You can also view the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

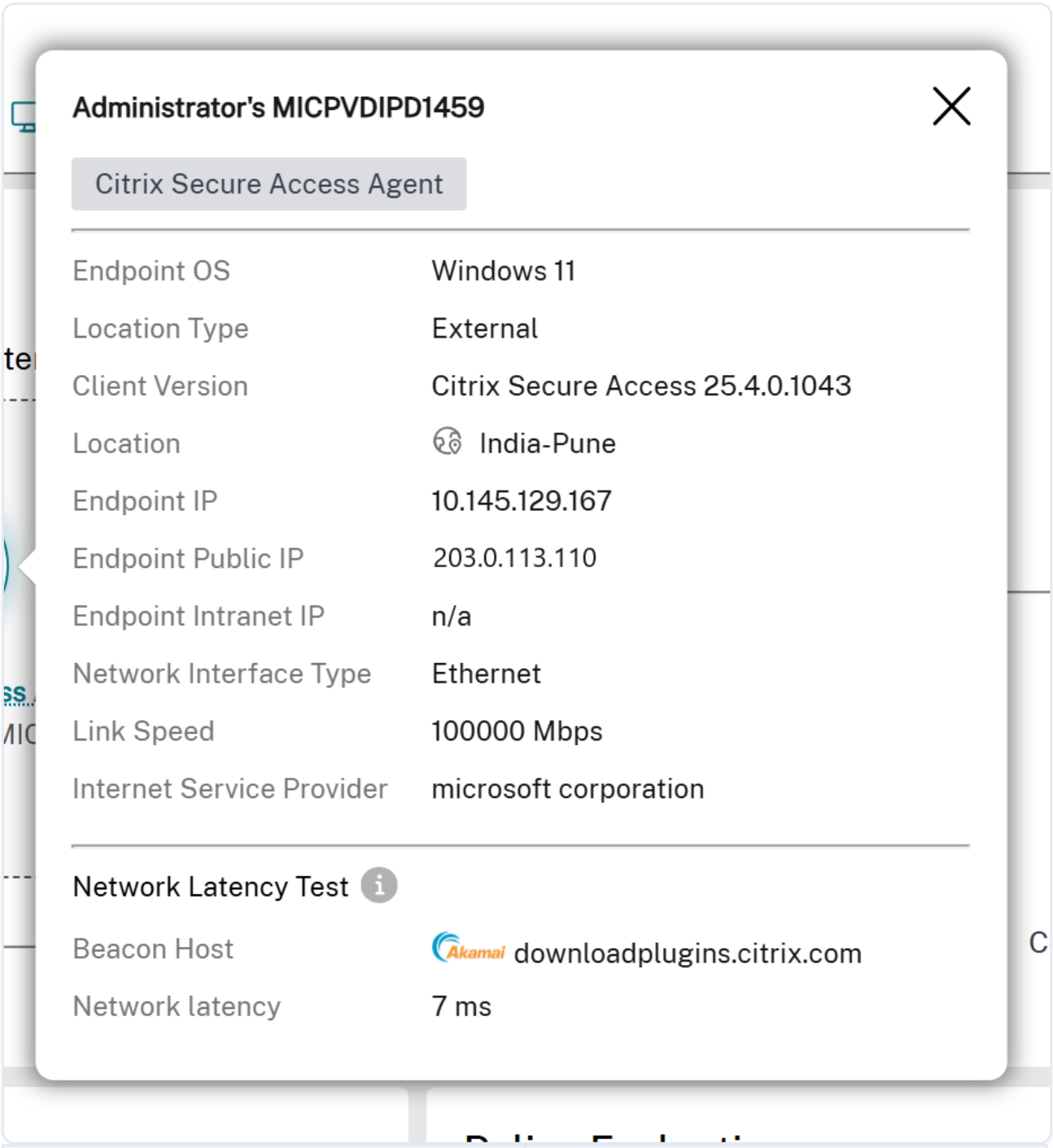
FIELD NAME	DESCRIPTION
	endpoint OS, endpoint IP, location type, localtion and network details.
Citrix Cloud	Displays the number of enumerated apps and the number of configured policies.
Policy evaluation	Displays the result of the policy that is set on the Secure Private Access app. The possible values are **Allowed**, **Denied**, **Access allowed with restrictions**, and **Error**.
Public network	Displays the type of apps and the status of app launch. The possible value for app types is Web/SaaS app. Similarly, the possible values for app launch statuses are **Allowed**, **Denied**, **Access allowed with restrictions**, and **Error**. You can also view the top level URL, app type, and app publishing.
Resource Location	Displays the type of apps and the status of app launch. The possible value for app types is TCP/UDP app. You can also view the top level URL, app type, and app publishing.

Endpoint details

Displays key information about the client device and network used to access the application. Hover over Endpoint to view detailed information.

The following figure displays a sample **Endpoint details** pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



FIELD NAME	DESCRIPTION
Endpoint OS	The operating system of the endpoint device.
Location type	The type of location from which the endpoint device is connecting. The possible values are Internal and External.
Client Version	The version of the Citrix Workspace app or Citrix Secure Access client installed on the endpoint device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD NAME	DESCRIPTION
Location	The geographical location of the endpoint device based on its IP address.
Endpoint IP	The private IP address of the endpoint device.
Endpoint Public IP	The public IP address of the endpoint device.
Endpoin Intranet IP	The intranet IP address of the endpoint device.
Network Interface Type	The type of network interface used by the endpoint device. The possible values are Ethernet, Wi-Fi, Cellular, and Other.
Signal Strength	The signal strength of the network connection on the endpoint device, measured in dBm.
Link Speed	The speed of the network connection on the endpoint device, measured in Mbps.
Internet Service Provider	The name of the Internet Service Provider (ISP) for the endpoint device.
Beacon Host	The hostname of the beacon server used for connectivity checks.
Network Latency	The round-trip time for data packets to travel from the endpoint device to the beacon server and back, measured in milliseconds (ms).

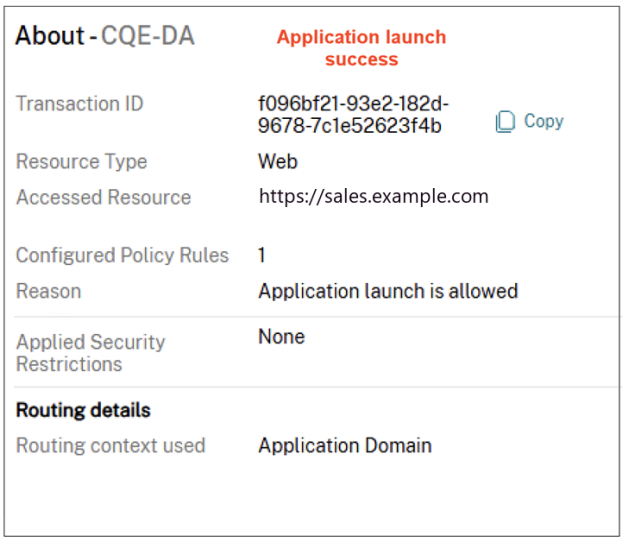
This information helps administrators identify the network path, troubleshoot connectivity issues, and correlate performance with specific endpoints. Fields are shown based on deployment type and available data.

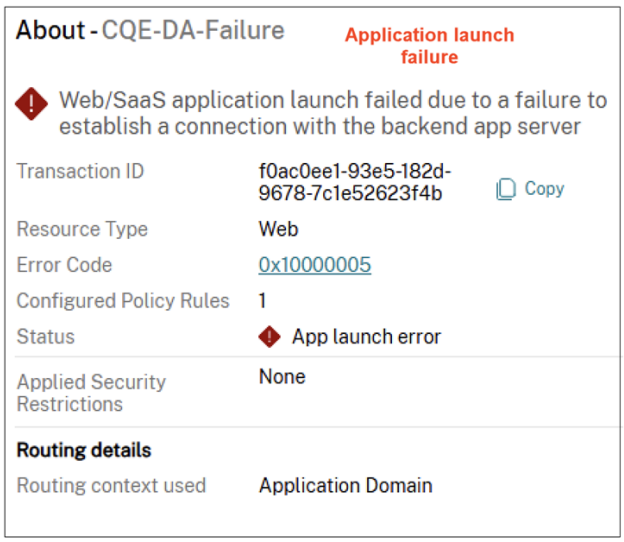
About pane

Displays additional information regarding the Web/SaaS, TCP/UDP and agentless apps for both the successfully launched apps and the failed apps. In cases where an app fails, the **About** pane shows the corresponding error code. Clicking this code redirects you to a documentation page detailing the cause and workaround. For other issues, you are directed to the Citrix support page.

The following figure displays a sample **About** pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





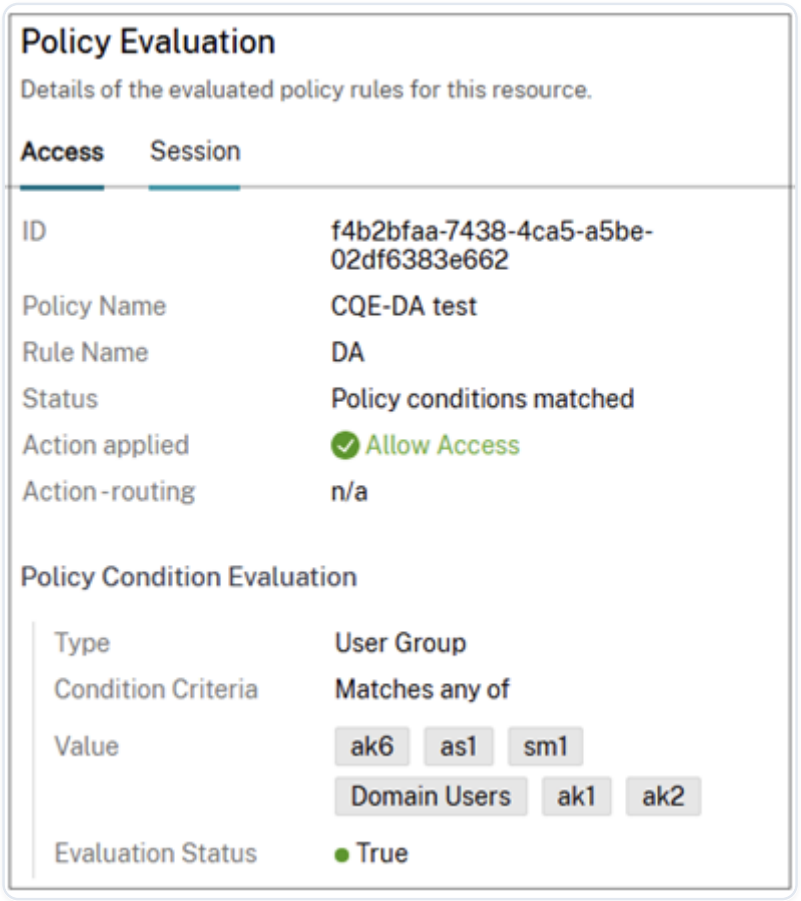
FIELD NAME	DESCRIPTION
Transaction ID	Citrix Transaction ID generated during the session or enumeration.
Resource Type	Displays the type of the resource. The possible values are Web, SaaS, TCP/UDP (Server to Client), and TCP/UDP (Client to Server).
Accessed Resources	The data that appears in the **Accessed Resources** field varies depending on the app type.
	SaaS apps - URL or the app FQDN
	TCP/UDP – IP address/FQDN, port, and protocol
	Web app (launched via Citrix Secure Access client) - FQDN, port, and protocol
	Web app (launched via Citrix Workspace) - URL
	Agentless apps - URL of the application
Configured Policy Rules	The number of policies that are used within a session or enumeration.
Reason	The result of the analysis of the session or enumeration activity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD NAME	DESCRIPTION
Applied security restrictions	Displays the security restrictions that are enforced on this app.
Routing context	Displays the policy type (access policy, session policy, or application domain) applied during routing. The routing context helps identify the hierarchy (access policy > session policy > default application domain) influencing routing decisions.
	For session policy, the View details link provides additional details about the session policy.

Policy Evaluation pane

Displays information related to the policy, such as rules, actions, and conditions in the **Access** and **Session** tabs. The access policy details can be viewed under the **Access** tab. The session policy details can be viewed in the **Session** tab.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD NAME	DESCRIPTION
ID	Citrix transaction ID
Policy Name	The name of the policy that is associated with the application. If there are multiple policies, the first policy that is matched with the set condition appears.
Rule name	The rule name configured within the policy.
Status	Results of the policy evaluation
Action applied	The action applied on the application based on the policy evaluation results. For example, deny access.
Action routing	Displays the routing path (Direct, Internal via connector, Internal via gateway) that a user's request takes through the Secure Private Access service. For the mapping between these values and the diagram terms used in Chrome Enterprise Premium topology, see Application route vocabulary.
Type	The type of the policy condition.
Condition Criteria	The condition criteria of the policy applied in the session or during enumeration.
Value	Results of the condition evaluation.
Evaluation status	Status of the policy condition evaluation result. The different values are Allowed, Denied, Access allowed with restrictions, and Error.

NOTE:

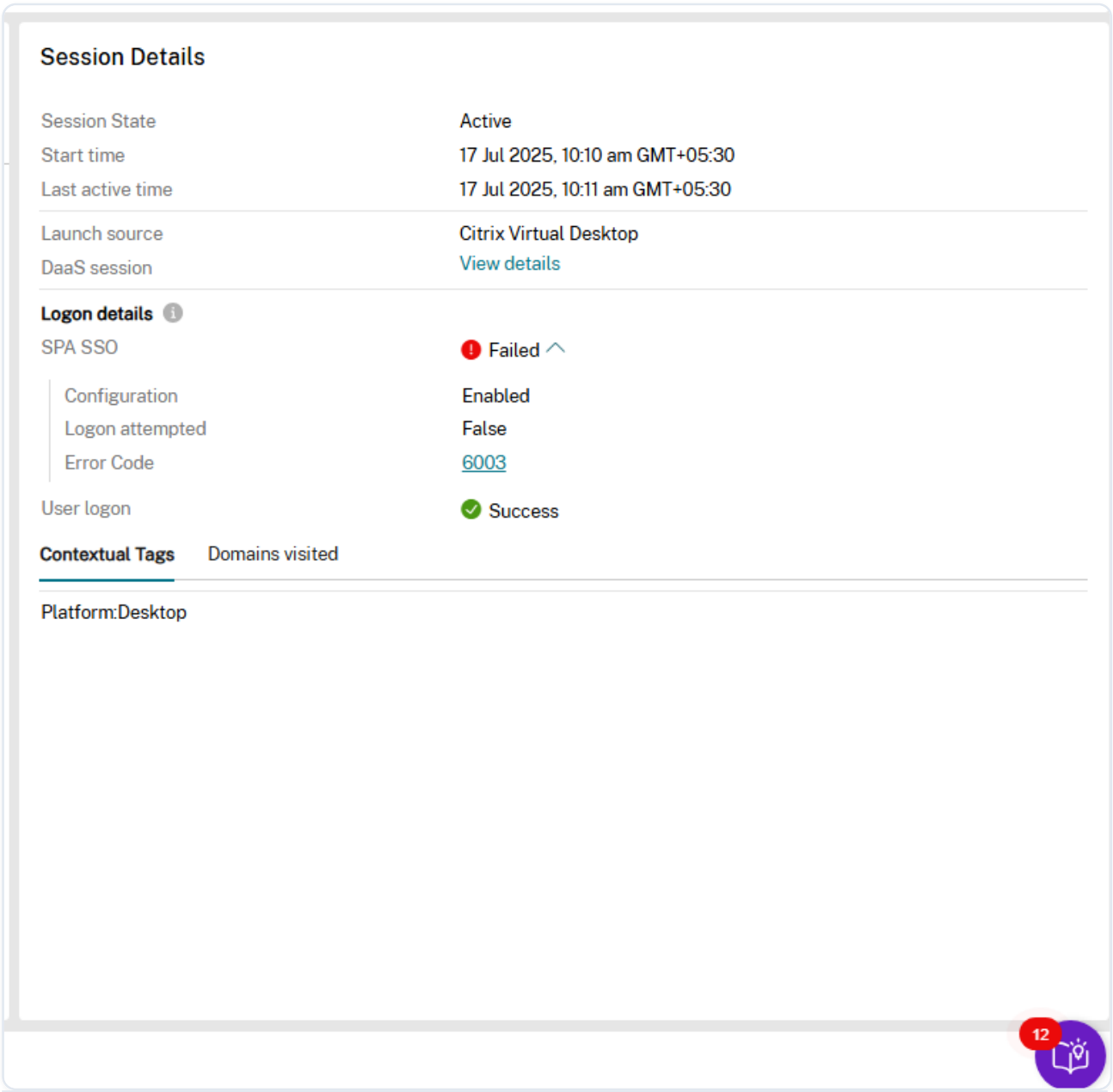
The **Application Name**, **Application Type**, **Policies**, and **Security Controls** fields can show values carried over from an enumeration event when the originating app launch event does not include those values. The **Data path** field can also render empty when the source event does not specify it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session Details pane

For a failed session, the reason for session failure is displayed. For a successful session, additional details related to the session are displayed.

The **Session Details** pane remains empty for apps clicked from the **Available Apps** tab, as app enumeration is not associated with a session.



FIELD NAME	DESCRIPTION
Session state	Displays the state of the session whether it is active or inactive.
Start time	Displays the session start time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD NAME	DESCRIPTION
Last active time	Displays the last active time of the successful session.
Launch source	Displays the source from where the Secure Private Access session is launched.
DaaS Session	Displays details of the DaaS session. This field appears only in case of a single session or multi-session VDA.
Logon details	
SPA SSO	Displays whether the single sign on to Secure Private Access session is success or failure.If failed, user has to login manually.
Configuration	Displays the configuration status of single sign on to Secure Private Access session. If not configured, the details will be shared to the admin.
Logon attempted	Displays the logon attempt status of single sign on to Secure Private Access session.
Error code	Displays the error code when the logon attempt of single sign on to Secure Private Access session is failed. The possible error codes are: 6007 and 6003.
	6003- Error retrieving the Secure Private Access single sign-on handle from the Broker Agent service.
	6007- Failed to login to Secure Private Access.
User logon	Displays the manual user log on status to Secure Private Access session.
Gateway Virtual IP	Displays the virtual IP address of the gateway to which the successful session is connected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

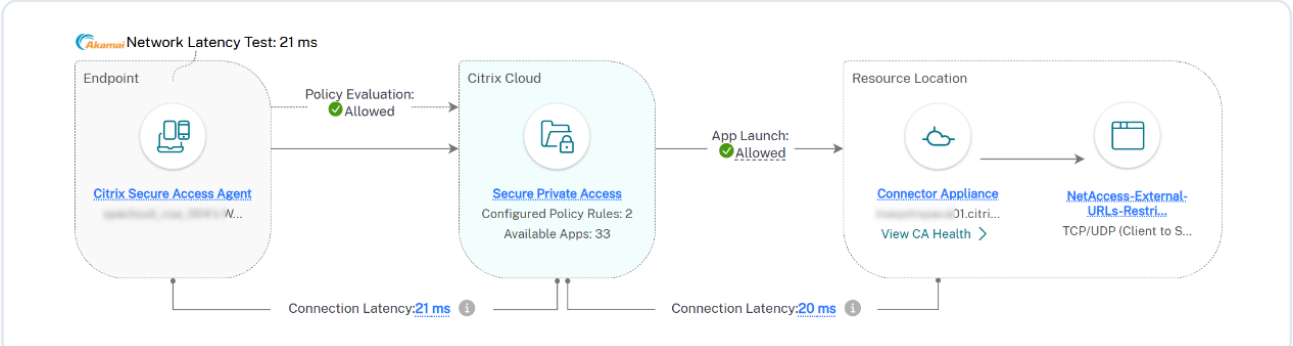
FIELD NAME	DESCRIPTION
	This field is applicable only for hybrid data path deployment.
Contextual Tags	Displays the contextual tags. The contextual tag on the Secure Private Access plug-in is the name of a NetScaler® Gateway policy (session, preauthentication, EPA) that is applied to the sessions of the authenticated users.
Domains visited (Internal)	Displays the internal domains accessed using the successful session.
Domains visited (External)	Displays the external domains accessed using the successful session.
	The **Domains Visited** field is applicable only for the Web/SaaS apps and is updated only after 15 minutes, as the Citrix Enterprise Browser clients on macOS and Windows send session activity every 15 minutes.

NOTE:

The Session Details column pane remains empty for apps clicked from the Available Apps tab, as app enumeration is not associated with a session.

Hop by hop latency

The latency details for each hop in the application topology are displayed over each path. This information helps admins triage and isolate performance or slowness issues across the multiple hops.



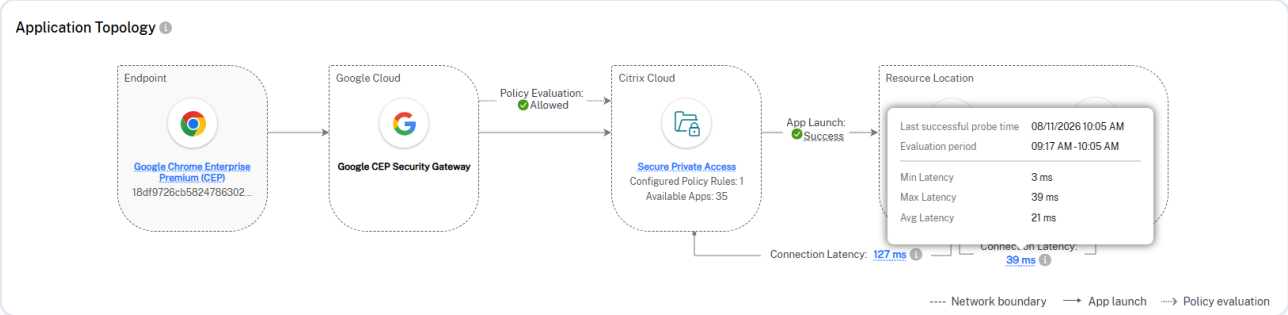
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Hop-by-hop latency information is only available for apps launched via Secure Access Client version V25.7.1.x or later.
- Latency information from the client to SPA is displayed for the last hour only. If the session has not been active within the past hour, no data will be shown.

CONNECTOR APPLIANCE TO BACKEND APPLICATION LATENCY

When a Secure Private Access session reaches its backend through a Connector Appliance, the topology shows a **Connection Latency** label on the link between the Connector Appliance and the backend application. This value is the round-trip time (RTT) between the Connector Appliance and the backend, measured using periodic synthetic probes. It completes the hop-by-hop view, alongside the latency shown on the earlier hops. Because the Connector Appliance measures this hop directly, the reading does not depend on the endpoint client version.



The Connector Appliance records four values for this hop over the evaluation window (the past hour):

- **Minimum:** The lowest RTT measured in the window.
- **Maximum:** The highest RTT measured in the window.
- **Average:** The mean RTT across the window.
- **P90:** The 90th-percentile RTT.

The topology label displays the P90 value.

The Connector Appliance sends RTT probes every 15 minutes to the backend IP addresses that it has forwarded traffic to in the last 8 hours. If the session has had no backend activity in the past hour, no value is shown. Monitor keeps this latency data for 3 days.

Currently, the Connector Appliance to backend application latency appears for cloud deployments only. It might not appear for every eligible session yet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

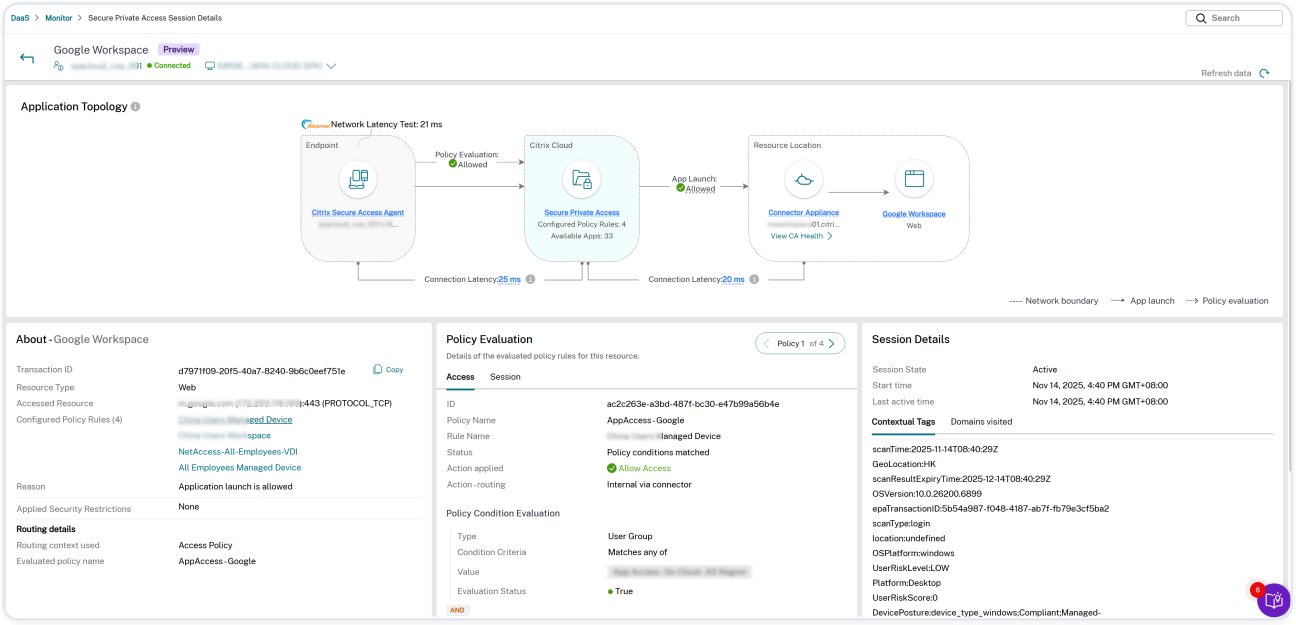
Hovering over the label shows the following tooltip: `Connection Latency is a synthetic metric (P90) measured over the evaluation window, collected periodically as probes between defined endpoints.`

NOTE:

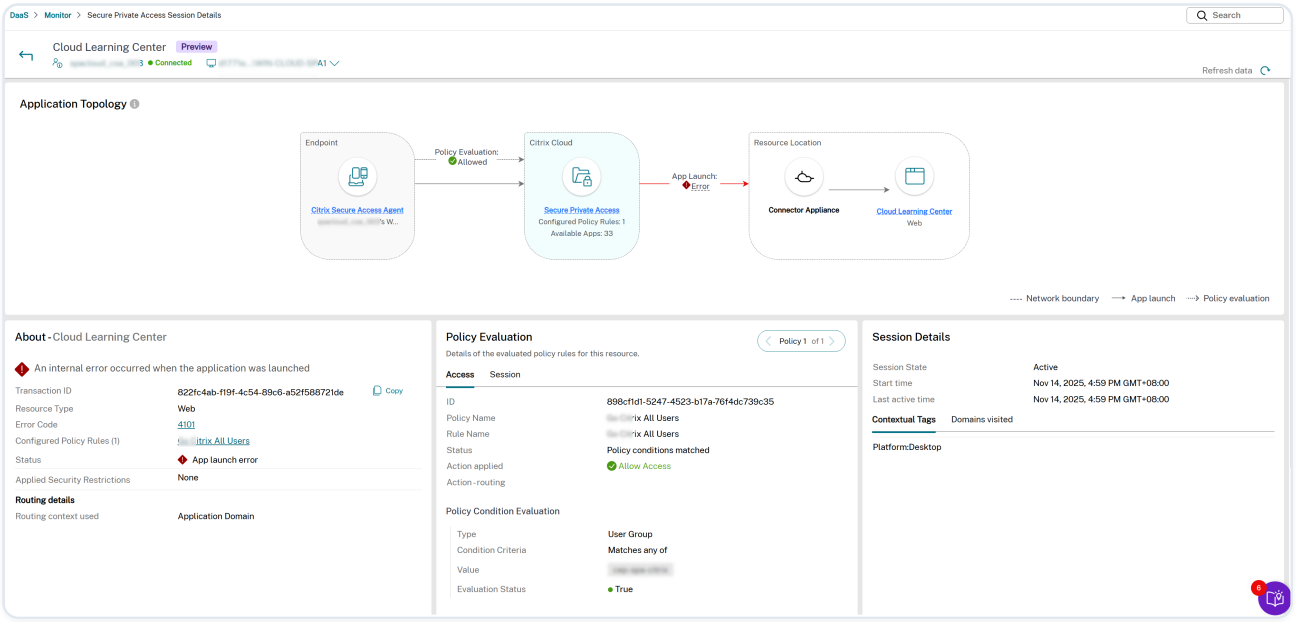
- A value of `-1` means the backend was unreachable from the Connector Appliance during the probe.
- A blank or **n/a** value means no probe data has been collected yet for that backend.
- If this hop shows high latency or `-1`, run an on-demand probe from the Connector Appliance to the backend to confirm reachability and isolate the failing stage. For more information, see Troubleshoot application reachability.

Sample topology diagrams for the various apps

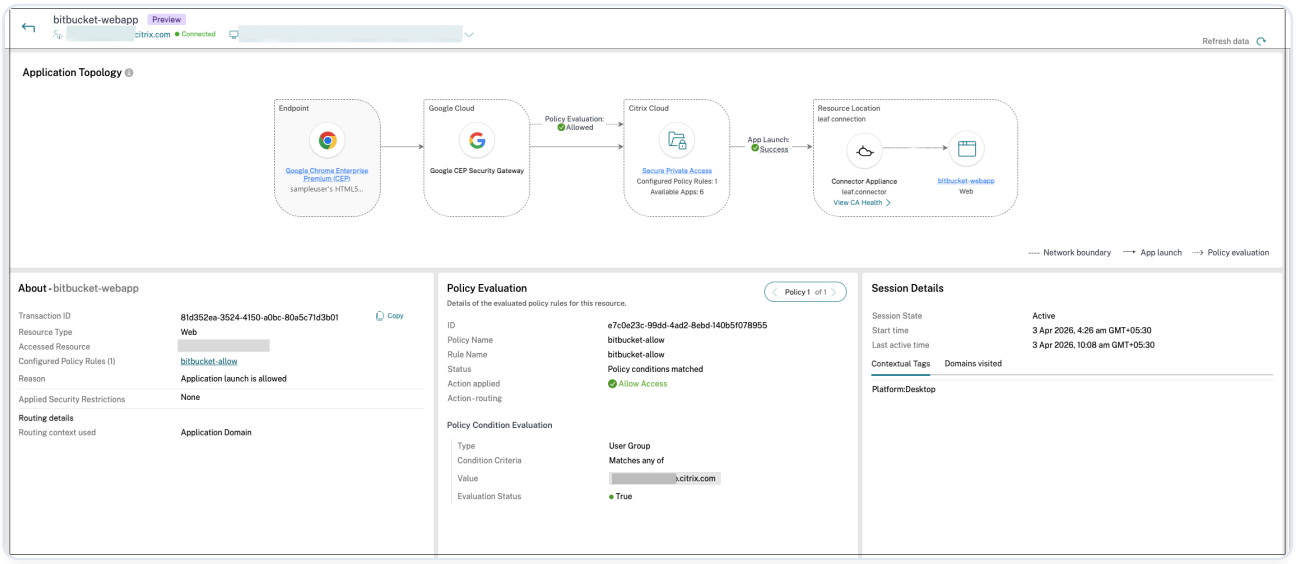
Web/SaaS apps - Success scenario:



Web/SaaS apps - Failure scenario:

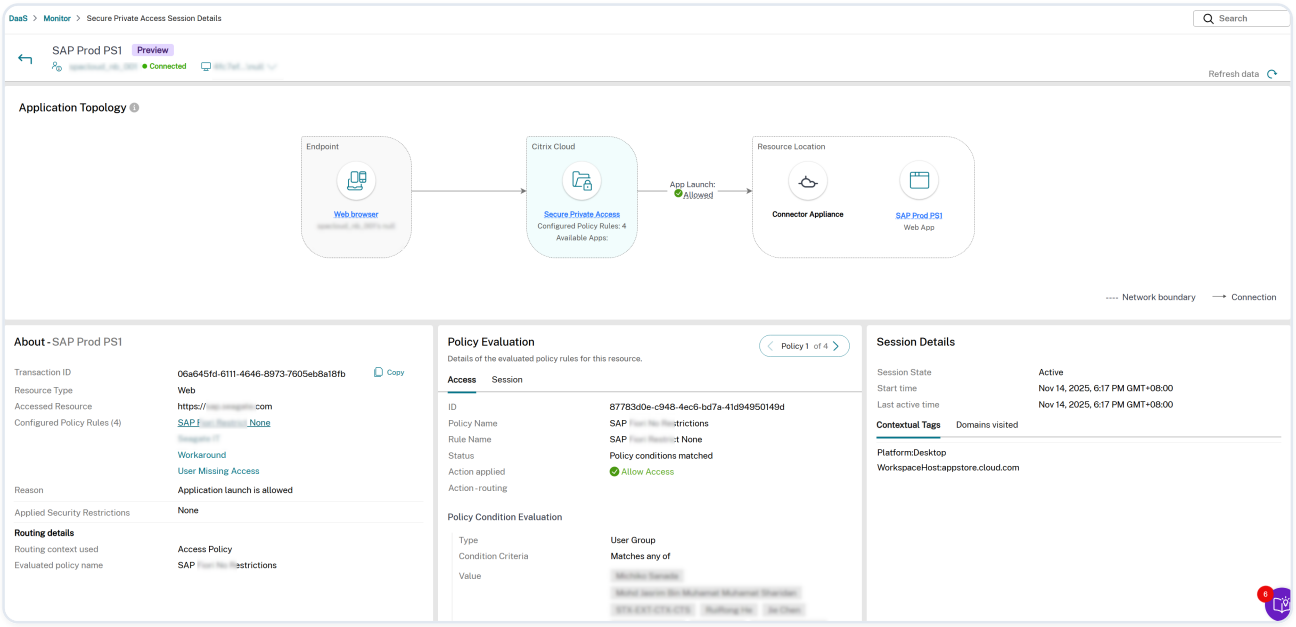


SaaS apps traffic routed through Google Secure Gateway:

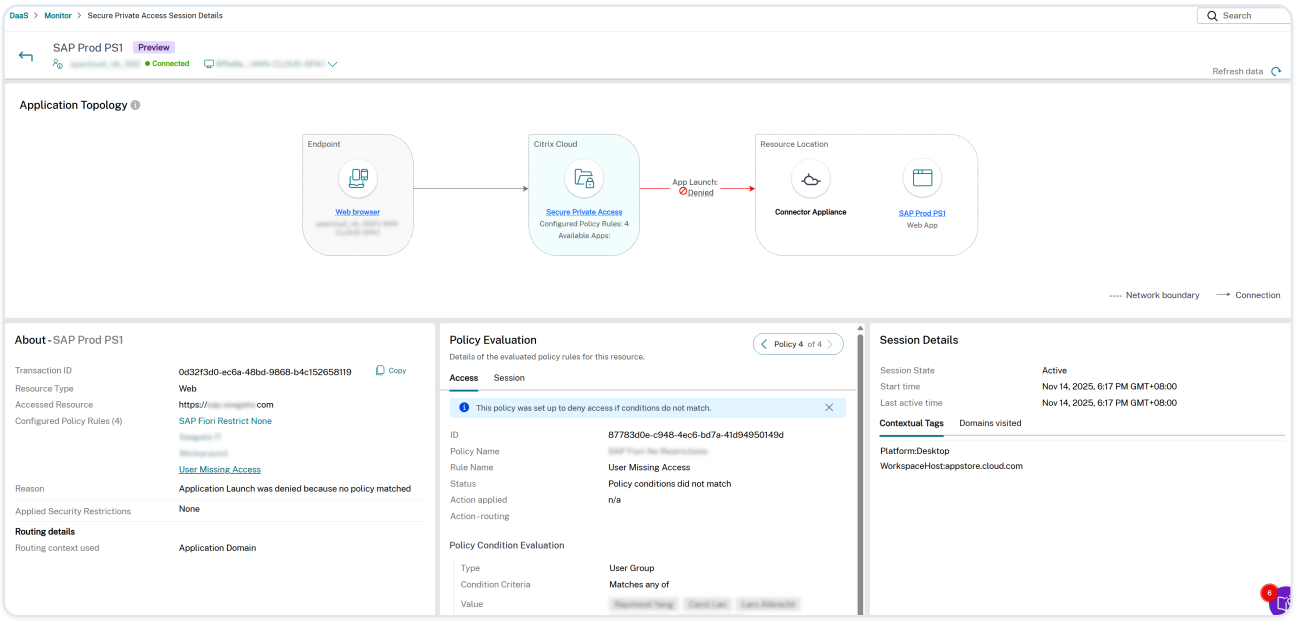


Agentless apps - success scenario:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

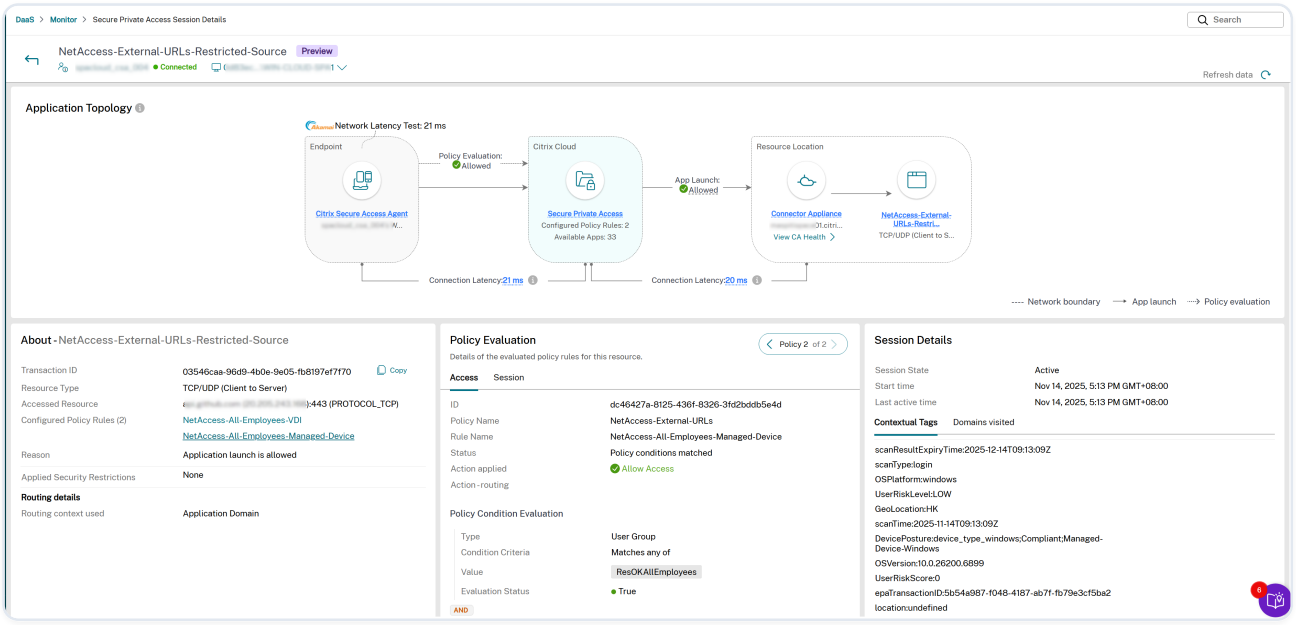


Agentless apps - Failure scenario:

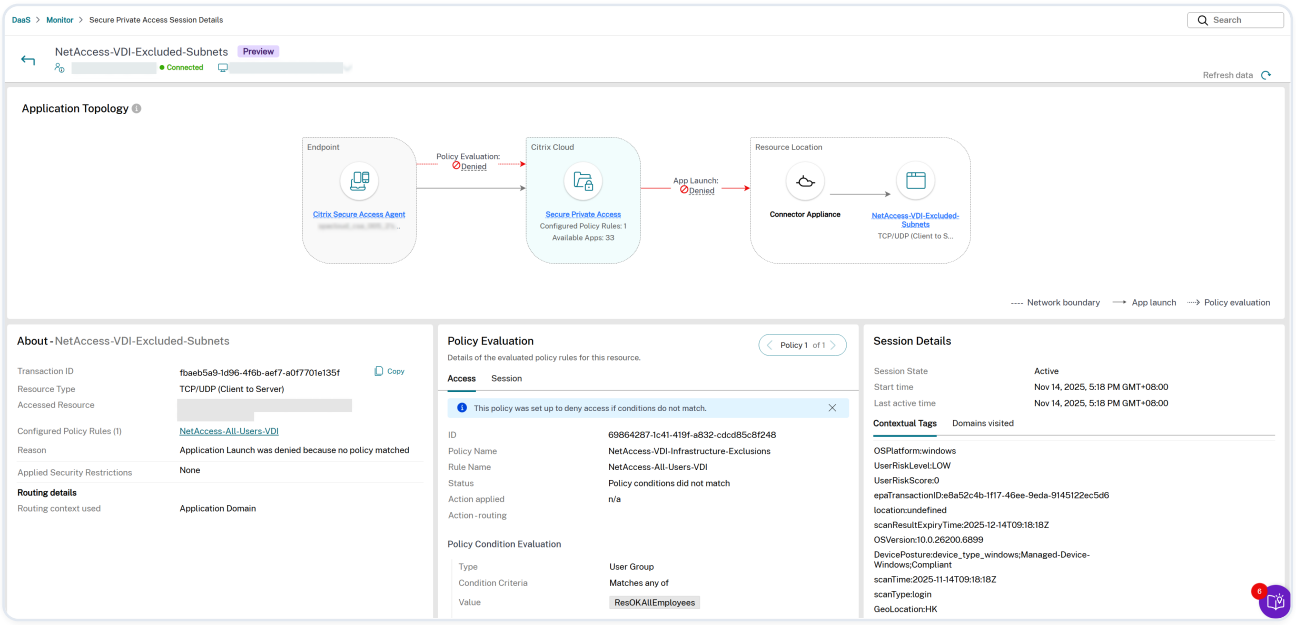


TCP/UDP apps - success scenario:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

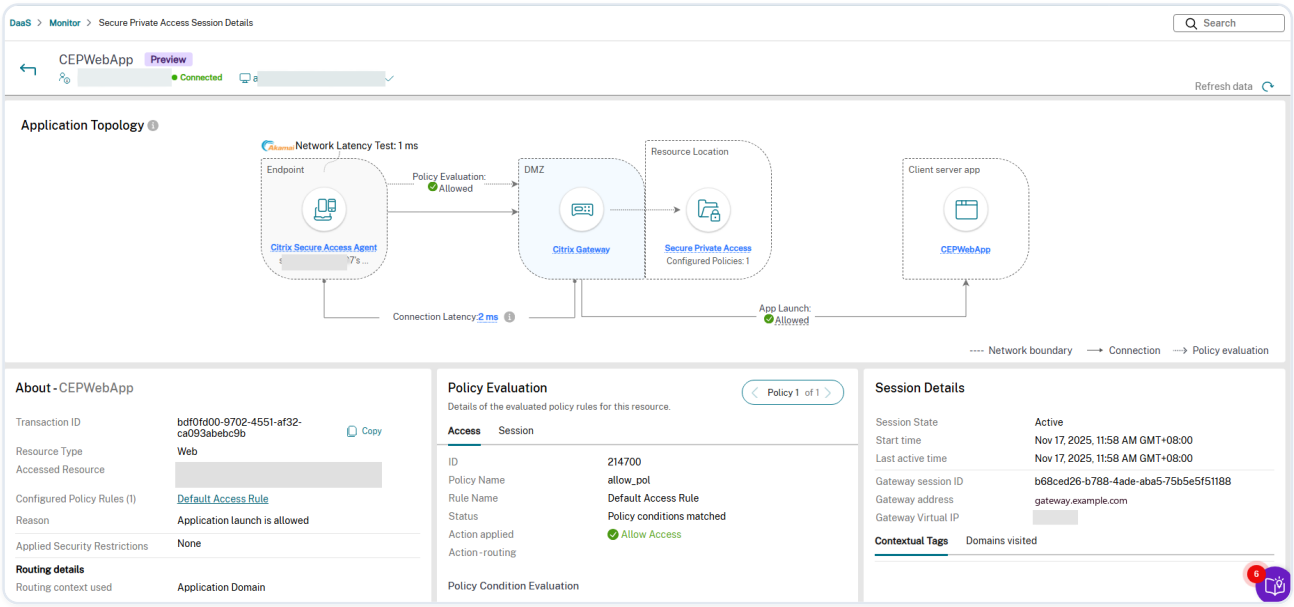


TCP/UDP apps - Failure scenario:



Hybrid deployment:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Application route vocabulary

The Chrome Enterprise Premium topology diagrams use the backend `applicationRoute` taxonomy, while the **Action routing** field on the Session Details page uses the routing labels shown in the Monitor UI. The following table maps the two.

DIAGRAM VOCABULARY (`APPLICATIONROUTE`)	ACTION ROUTING UI LABEL	MEANING
`internal`	Internal via connector	Traffic egresses through a Connector Appliance in the resource location.
`external`	Direct	Traffic egresses directly to the backend application, without traversing the Secure Private Access fixed-IP egress.
`external_fixed_ip`	Internal via gateway	Traffic egresses through the Secure Private Access gateway with a fixed egress IP for allow-listing at the destination.

Chrome Enterprise Premium topology variants

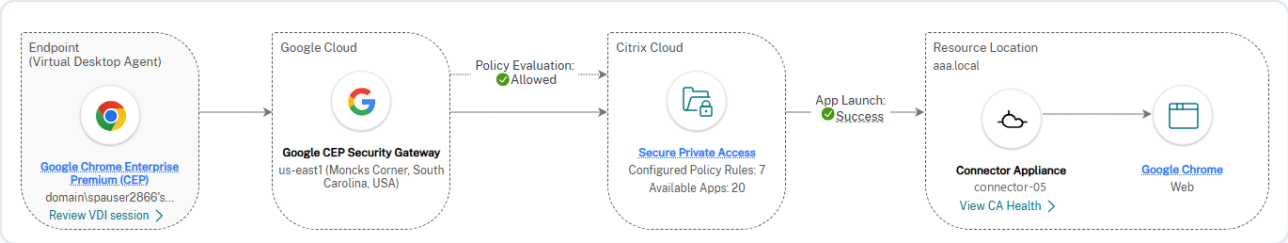
The Chrome Enterprise Premium topology has six variants, determined by the deployment type (cloud or hybrid) and the application route (`internal`, `external`, or `external_fixed_ip`) for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the launched app. A failed launch highlights the failing segment of the flow in a different color, as described under Application topology. For application-reachability triage steps, see Troubleshoot application reachability.

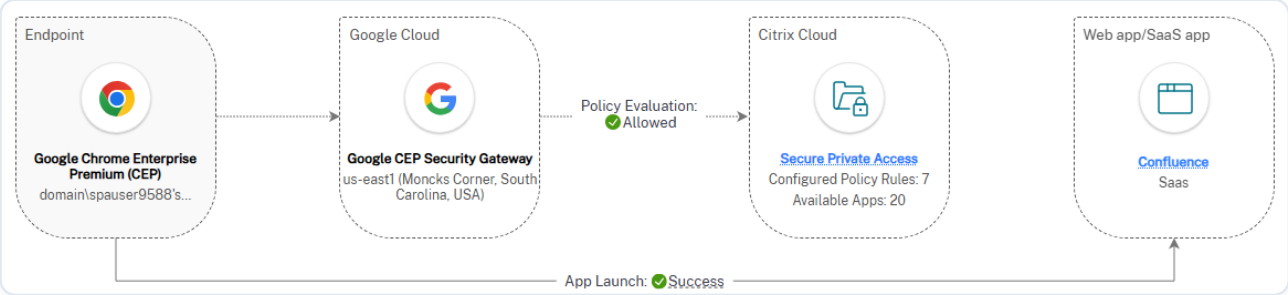
CLOUD DEPLOYMENT — INTERNAL ROUTE

A Chrome Enterprise Premium session in a cloud deployment uses the internal route when the destination app is reached through a Connector Appliance in the resource location. Traffic flows from the Chrome Enterprise Premium endpoint through Citrix Cloud to the Connector Appliance, and then to the internal backend application.



CLOUD DEPLOYMENT — EXTERNAL ROUTE

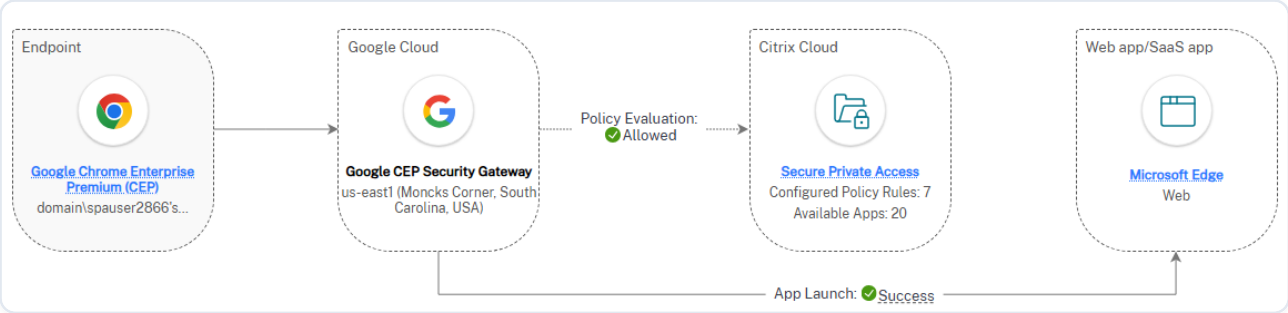
A Chrome Enterprise Premium session in a cloud deployment uses the external route when the destination app is reached directly, without traversing the Secure Private Access fixed-IP egress. Traffic flows from the Chrome Enterprise Premium endpoint through Citrix Cloud directly to the external backend application.



CLOUD DEPLOYMENT — EXTERNAL FIXED IP ROUTE

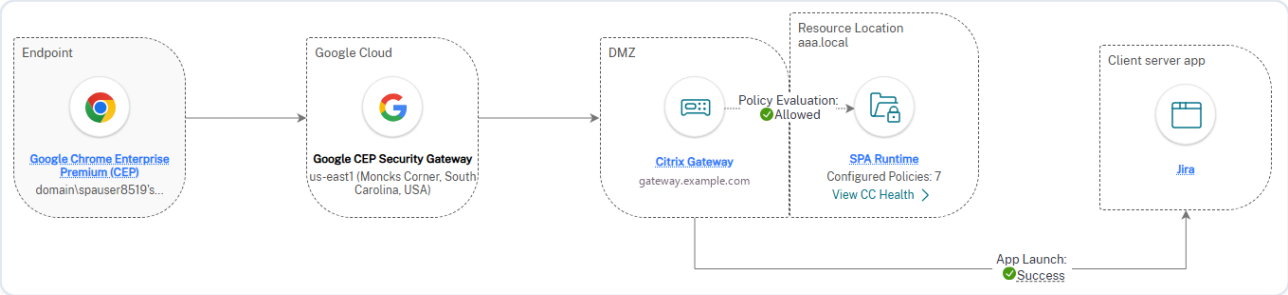
A Chrome Enterprise Premium session in a cloud deployment uses the external fixed IP route when the destination requires a known egress IP for allow-listing. Traffic flows from the Chrome Enterprise Premium endpoint through Citrix Cloud and the Secure Private Access fixed-IP egress to the external backend application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



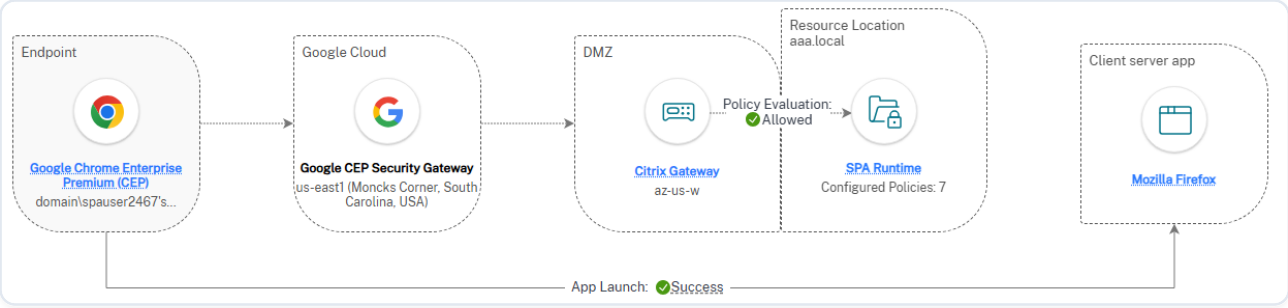
HYBRID DEPLOYMENT — INTERNAL ROUTE

A Chrome Enterprise Premium session in a hybrid deployment uses the internal route when the destination app is reached through a Connector Appliance in the resource location. Traffic flows from the Chrome Enterprise Premium endpoint through the on-premises Citrix Gateway to the Connector Appliance, and then to the internal backend application.



HYBRID DEPLOYMENT — EXTERNAL ROUTE

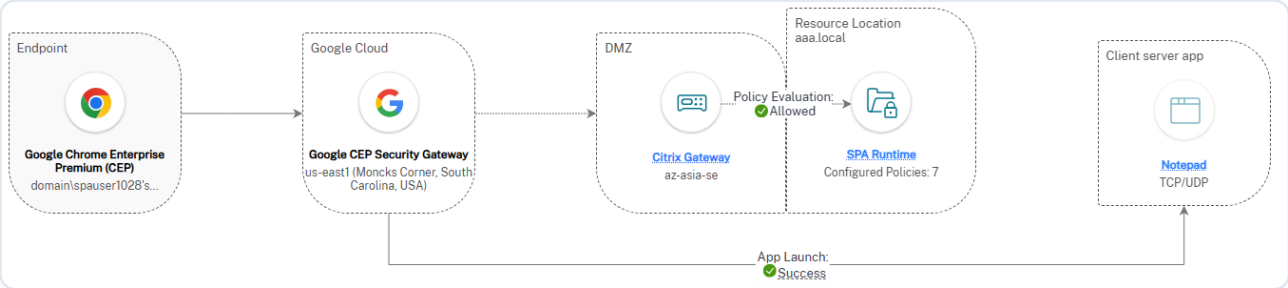
A Chrome Enterprise Premium session in a hybrid deployment uses the external route when the destination app is reached directly, without traversing the Secure Private Access fixed-IP egress. Traffic flows from the Chrome Enterprise Premium endpoint through the on-premises Citrix Gateway directly to the external backend application.



HYBRID DEPLOYMENT — EXTERNAL FIXED IP ROUTE

A Chrome Enterprise Premium session in a hybrid deployment uses the external fixed IP route when the destination requires a known egress IP for allow-listing. Traffic flows from the Chrome Enterprise Premium endpoint through the on-premises Citrix Gateway and the Secure Private Access fixed-IP egress to the external backend application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create and manage alerts

You can set up alerts for proactively monitoring conditions and scopes of interest to you and reduce alert fatigue. Alerts can be configured with severity, re-alert intervals, notification mediums, and follow the alert lifecycle supported in the product.

For more information, see the following:

- Alerts
- Advanced alert policies

Support for Chrome Enterprise Premium

Citrix Monitor supports Chrome Enterprise Premium (CEP) for Secure Private Access, enabling comprehensive monitoring and troubleshooting of Web/SaaS app sessions launched using Chrome Enterprise across devices.

Key features:

- User session search and filtering: Search and filter CEP user sessions across devices using the Client Type filter on the Filters page.
- Session activity review: View session activity, user profile enumerations, and app launches for CEP users.
- Session details and topology: Access the Session Details panel to review app launch transaction topology, including backend components (SPA PoP, Connector Appliance, and Client).
- Access policy triage: Analyze access policy outcomes, including denial errors, for CEP sessions.
- Visibility across Filters page: View detailed CEP session and application data, including launch errors, directly in the topology workflow.
- Domain and launch data collection: Collect and display data on domains visited (internal, external, direct, and bookmarked access) and app launch events.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

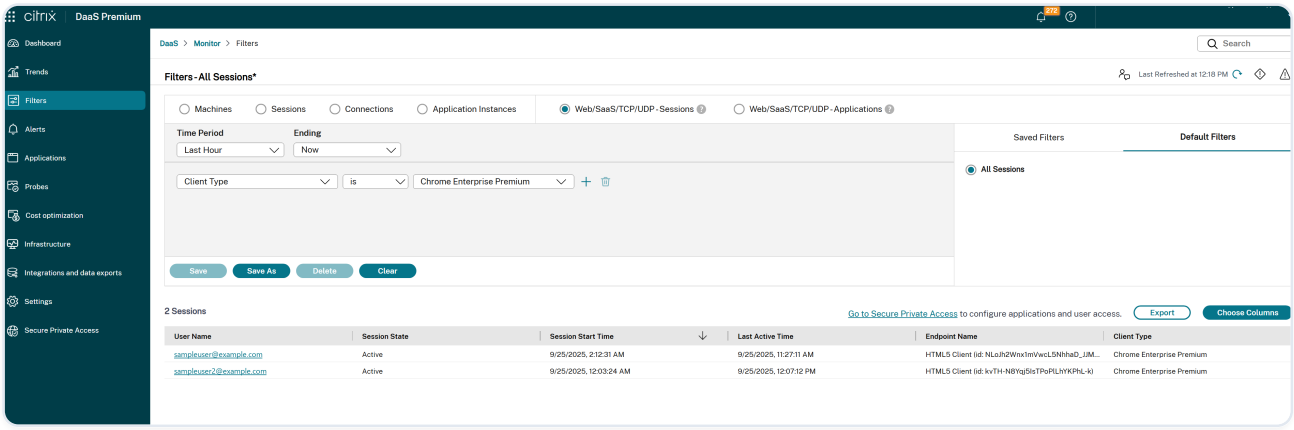
- Session lifecycle visibility: Monitor session lifecycle, heartbeats, and events with up to 7 days of historical data.
- Data parity: Ensure consistent data and visibility for all launch scenarios—Citrix Workspace app, CEP direct, SPA hybrid, and SPA cloud deployments.

NOTE:

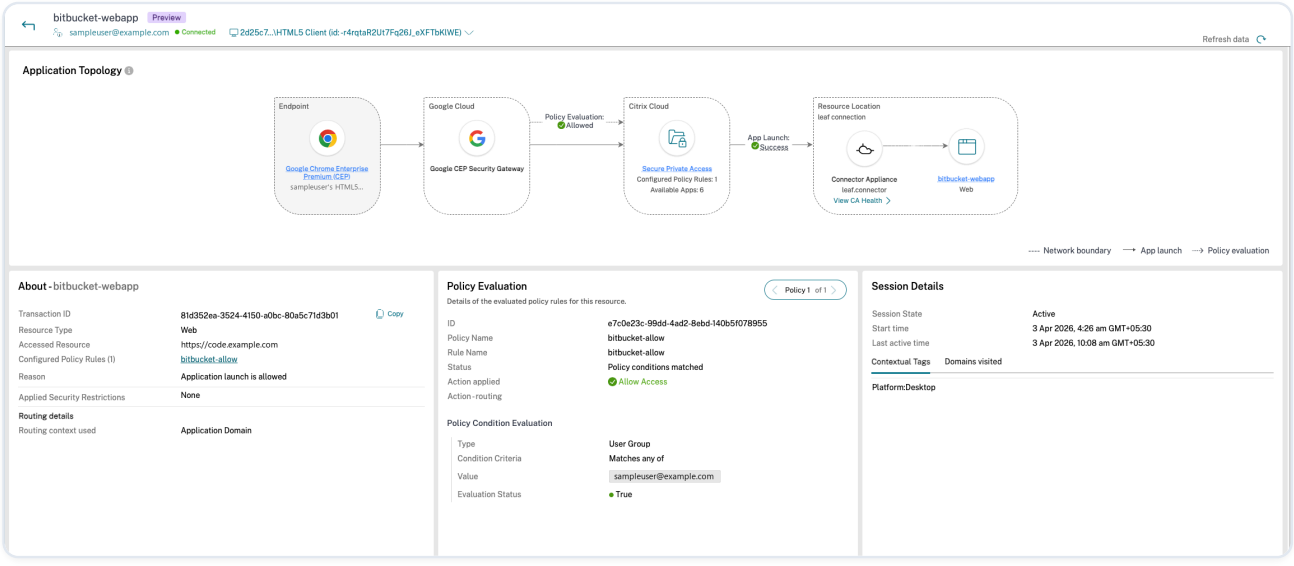
To monitor and troubleshoot Web/SaaS app sessions launched using Chrome Enterprise, ensure that you have the Chrome Enterprise Premium license. For more information about Chrome Enterprise Premium, see Chrome Enterprise.

View a session launched using Chrome Enterprise Premium in Filters page

You can search for the Chrome Enterprise Premium sessions from the **Filters** page, where the Client Type filter is available to locate specific sessions launched using Chrome Enterprise Premium.



The Activity Manager Page provides a complete view of app launch transactions, access policy outcomes, and launch errors, along with domain visited data and session lifecycle events.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Observability for multi-session VDA

The observability for multi-session VDA feature enhances the monitoring and troubleshooting capabilities for Secure Private Access sessions within a multi-user VDA environment. This feature empowers Citrix Helpdesk Administrators to monitor Secure Private Access sessions, troubleshoot issues, and gain insights into app launches and user transactions in case of a multi-session VDA.

Key features:

- Enhanced observability: Administrators can monitor Secure Private Access sessions, including app launches and enumerations, within the Citrix Director interface. This includes detailed views of enumeration and app launch issues.
- User context tracking: The feature maintains user context for apps accessed in a shared VDA environment, ensuring accurate session data visibility for each user.
- Error insights: Captures and displays Single Sign-On (SSO) failures, error codes (e.g., 6003, 6007), and troubleshooting steps to resolve issues.
- Session search: Administrators can search for sessions, apps, and user transactions using the same workflow as for VDI sessions and apps.
- Cross-session navigation: Enables navigation between Secure Private Access sessions and VDA sessions for streamlined troubleshooting.

Supported scenarios:

- Multi-user VDA environment: Supports multiple concurrent user sessions accessing internal apps, SaaS apps, and web apps through the Citrix Secure Access client.
- Single session Desktop: Extends the same functionality to single-session desktops for consistent observability across environments.

Error handling:

- Error Code 6003: Error in retrieving the Secure Private Access single sign-on handle from the Broker Agent service.
- Error Code 6007: Failed to login to Secure Private Access.
- Troubleshooting Guidance: Provides detailed error descriptions and links to troubleshooting steps within the Citrix Monitor.

For more information, see Citrix Secure Access client failed to do SSO in the Citrix Secure Private Access documentation.

Requirements:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Secure Access Version: Requires Citrix Secure Access version 25.2.1.18 or later for Windows.
- DaaS Service: The DaaS service must be accessible for troubleshooting Secure Private Access sessions using Citrix Monitor.
- CAS Deployment: CAS deployment must be available in the Citrix Cloud region where the customer is onboarded.
- The Citrix Secure Access agent is auto-installed and provisioned on the VDI.
- Secure Private Access sessions are initiated for internal web apps, TCP/UDP apps, and SaaS apps routed through internal connector appliances.

The Observability for multi-session VDA feature provides administrators with powerful tools to monitor, troubleshoot, and manage Secure Private Access sessions in a multi-user VDA environment. By offering detailed insights and streamlined workflows, this feature enhances the overall management experience and ensures efficient resource utilization.

Troubleshoot application reachability (Connector Appliance to backend app)

When a Web, SaaS, or TCP/UDP application that is delivered through Secure Private Access™ fails to launch, the cause is often a network problem between the Connector Appliance and the backend application server. Until now, administrators had no easy way to confirm whether the Connector Appliance could actually reach the backend, or to see exactly where the connection broke.

The **Run probe** option in Monitor solves this. It lets you trigger an on-demand network probe (a connectivity test) *from a specific Connector Appliance* to a backend host or application.

The probe walks through each stage of the connection—DNS resolution, TCP connection, TLS handshake, and the HTTP request—and reports the outcome and the time taken for each stage.

This helps you quickly confirm reachability and pinpoint the exact step that fails, without having to log on to the Connector Appliance console.

You can start a probe from two places in Monitor:

- The **Infrastructure** view, where you choose any monitored Connector Appliance and probe an arbitrary host or application.
- The **Application Topology** view of a Secure Private Access session, where the probe is offered in context when an app launch has failed to connect to its destination.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements

- Running a probe is an administrative troubleshooting action. You must sign in to Monitor as an administrator with full administrator permissions. The **Run probe** option isn't available to help desk administrators.
- You must have Secure Private Access entitlement to trigger a probe.
- The Connector Appliance must be monitored in the **Infrastructure** view. For more information, see Infrastructure monitoring.
- To start a probe from the topology view, you need both Citrix DaaS™ and Secure Private Access entitlements. For more information, see Monitor and troubleshoot Secure Private Access.

Probe protocols and inputs

When you start a probe, you choose the **Protocol** that matches the backend you want to test. The protocol determines which connection stages are tested and which target details you provide.

PROTOCOL	WHAT IT TESTS	TARGET DETAILS TO PROVIDE
ICMP	Whether the backend host responds to a ping from the Connector Appliance.	Target host (IP address or host name). No port required.
TCP	DNS resolution and whether a TCP connection can be opened on the port.	Target host and port.
SSL/TLS	DNS resolution, TCP connection, and the TLS handshake (including certificate negotiation).	Target host and port.
HTTP	DNS resolution, TCP connection, and the HTTP request or response.	Application URL.
HTTPS	DNS resolution, TCP connection, TLS handshake, and the HTTPS request or response.	Application URL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

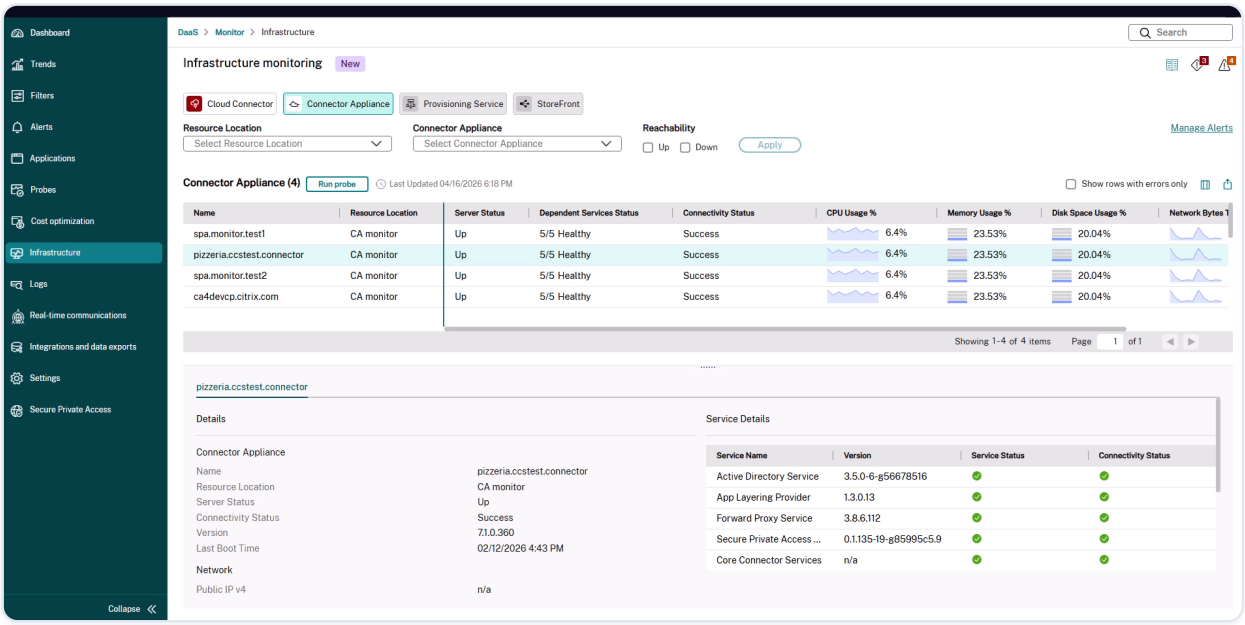
You can also choose whether the probe runs directly or through a proxy using the **Proxy** list:

- **Direct (no proxy)** – The Connector Appliance connects straight to the target.
- **\<proxy\>** – The Connector Appliance routes the probe through the selected proxy. The list shows the proxies (as `FQDN:PORT` or `IP:PORT`) that are available for the probe.

Run a probe from the Infrastructure view

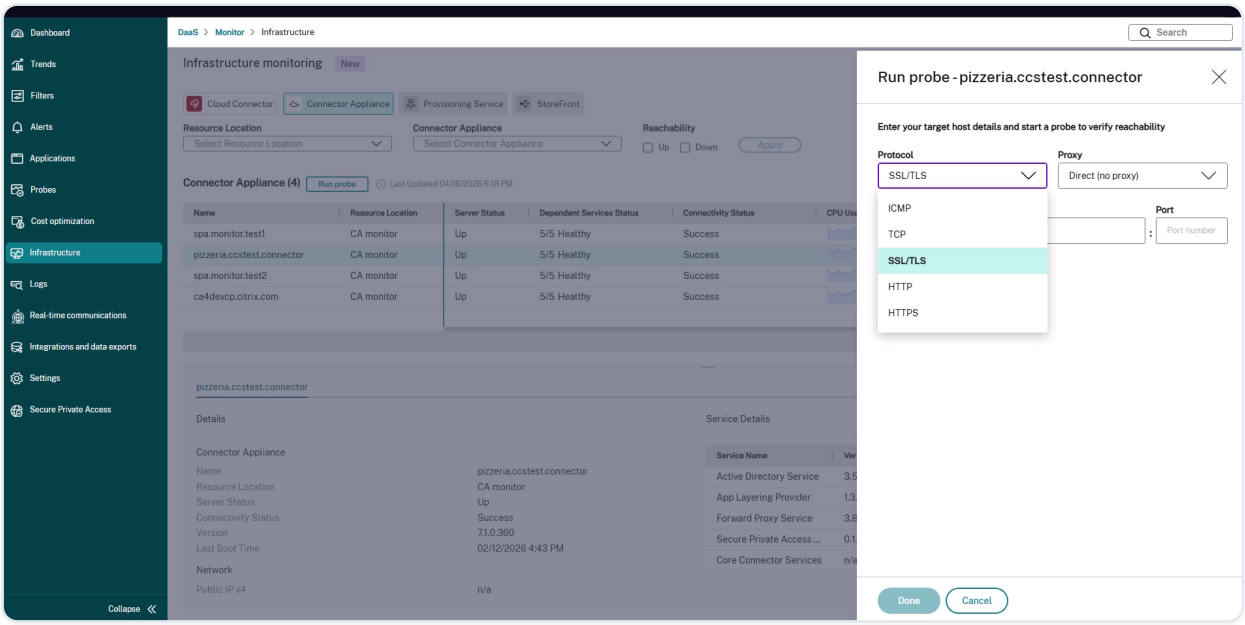
Use this method when you want to test reachability to any host or application from a chosen Connector Appliance—for example, to check a backend server that an app depends on.

1. In Monitor, go to **Infrastructure** and select the **Connector Appliance** tab. The table lists the monitored Connector Appliances with their server status, dependent services status, connectivity status, and resource usage.
2. Select the row of the Connector Appliance that you want to probe from, and then click **Run probe**.

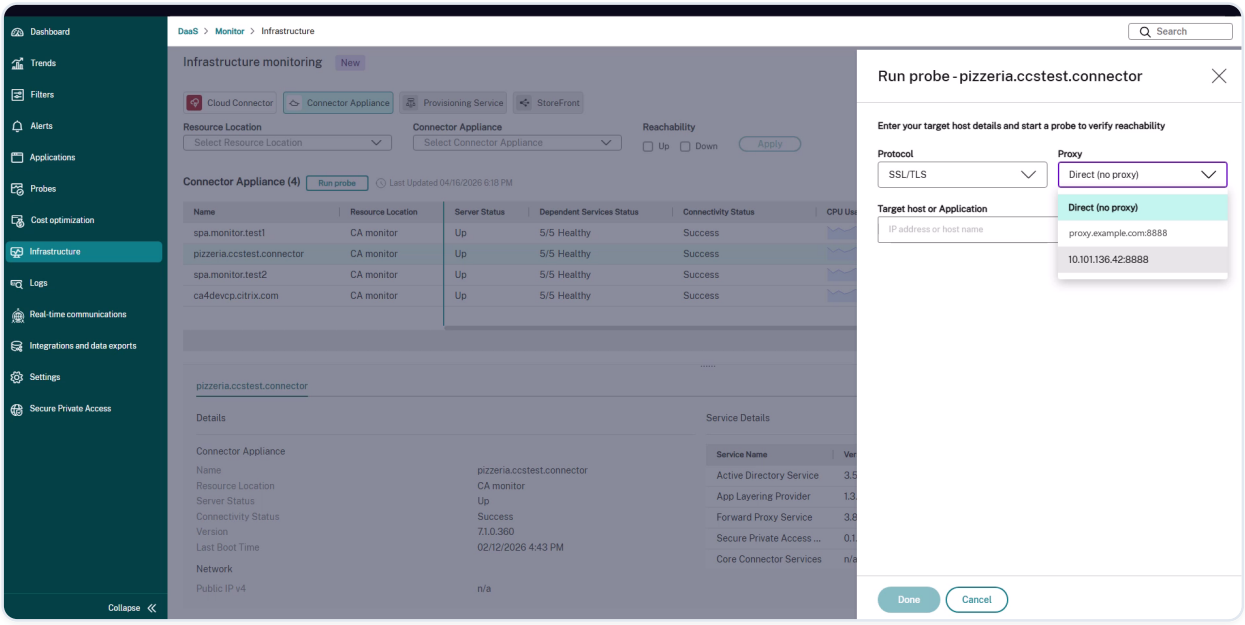


3. In the **Run probe** panel, select a **Protocol** and, if required, a **Proxy**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



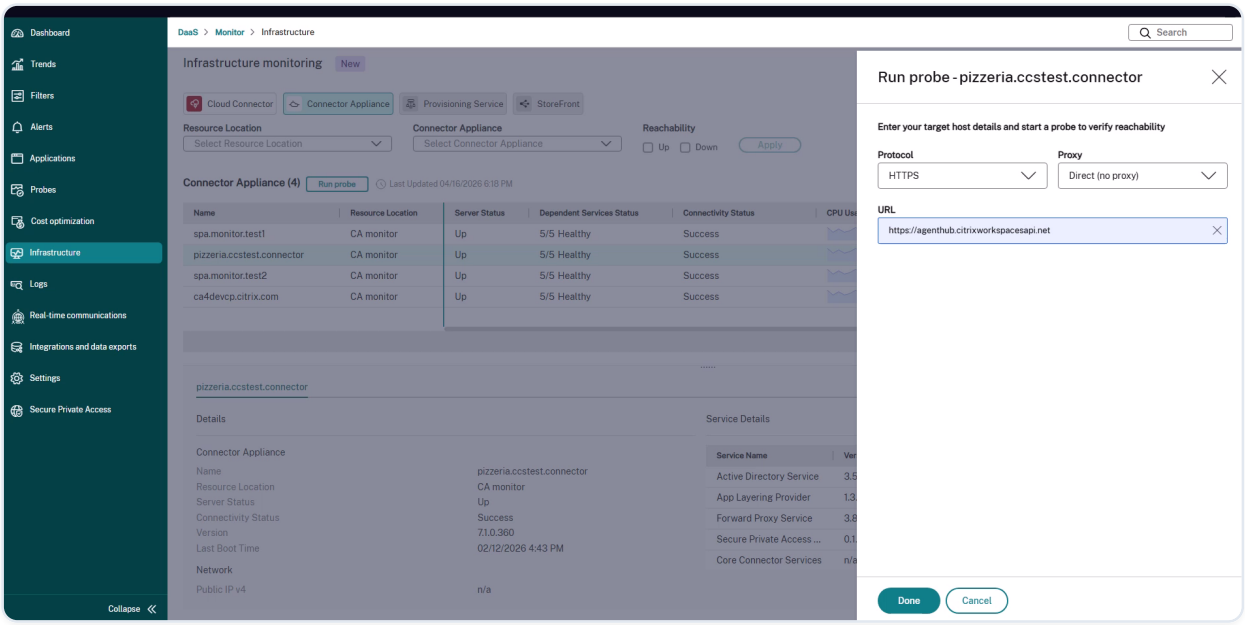
4. If you want the probe to go through a proxy, select it from the **Proxy** list. Otherwise, leave **Direct (no proxy)** selected.



5. Enter the target details for the protocol you selected:

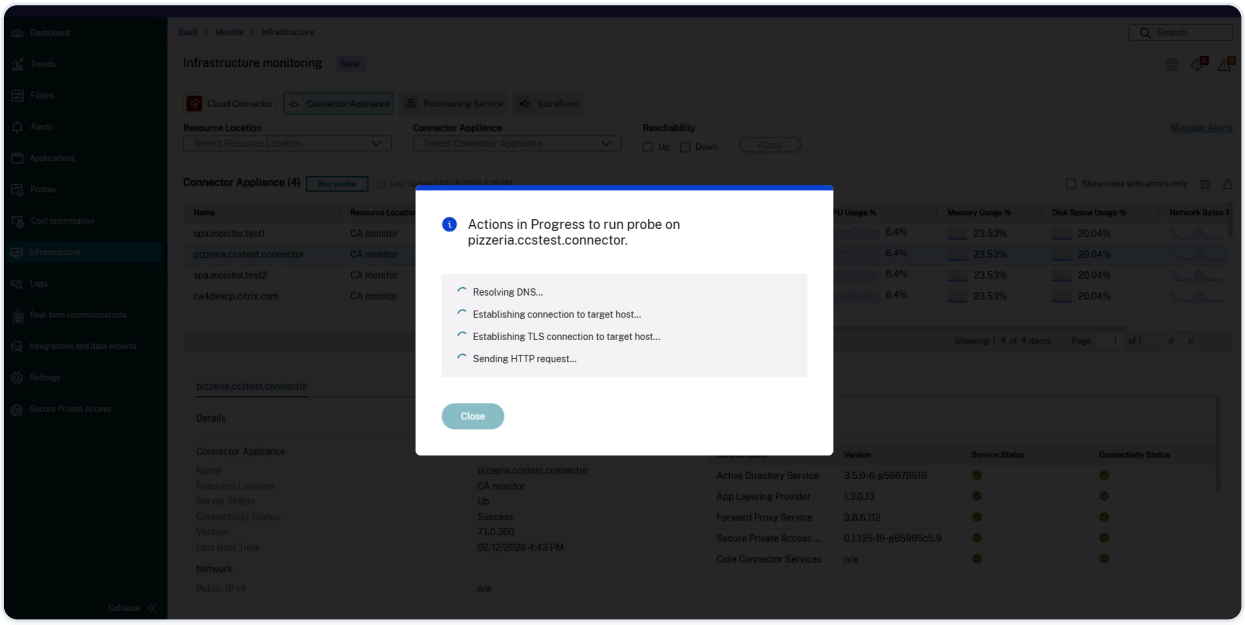
   - For **ICMP**, **TCP**, and **SSL/TLS**, type the **Target host or Application** (IP address or host name) and, where applicable, the **Port**.
   - For **HTTP** and **HTTPS**, type the application **URL**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Click **Done** to start the probe.

   Monitor shows the **Actions in Progress** dialog and updates each connection stage as it runs.



7. When the probe finishes, review the result. For more information, see Understand the probe results. Click **Close** to dismiss the dialog.

Run a probe from the Application Topology view

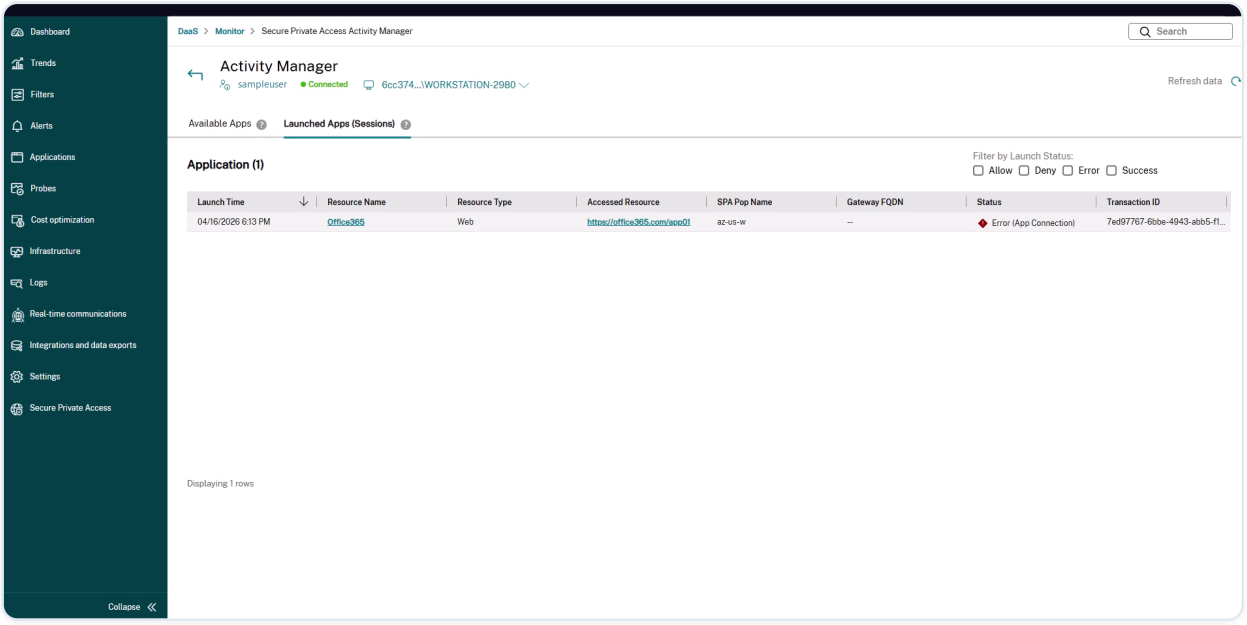
Use this method when you are already troubleshooting a failed Secure Private Access app launch. The probe is offered in context, with the protocol and target prefilled from the failing application.

When a Web, SaaS, or TCP/UDP app fails to launch because the Connector Appliance can't reach the backend, the **Application Topology** highlights the segment between the Connector Appliance

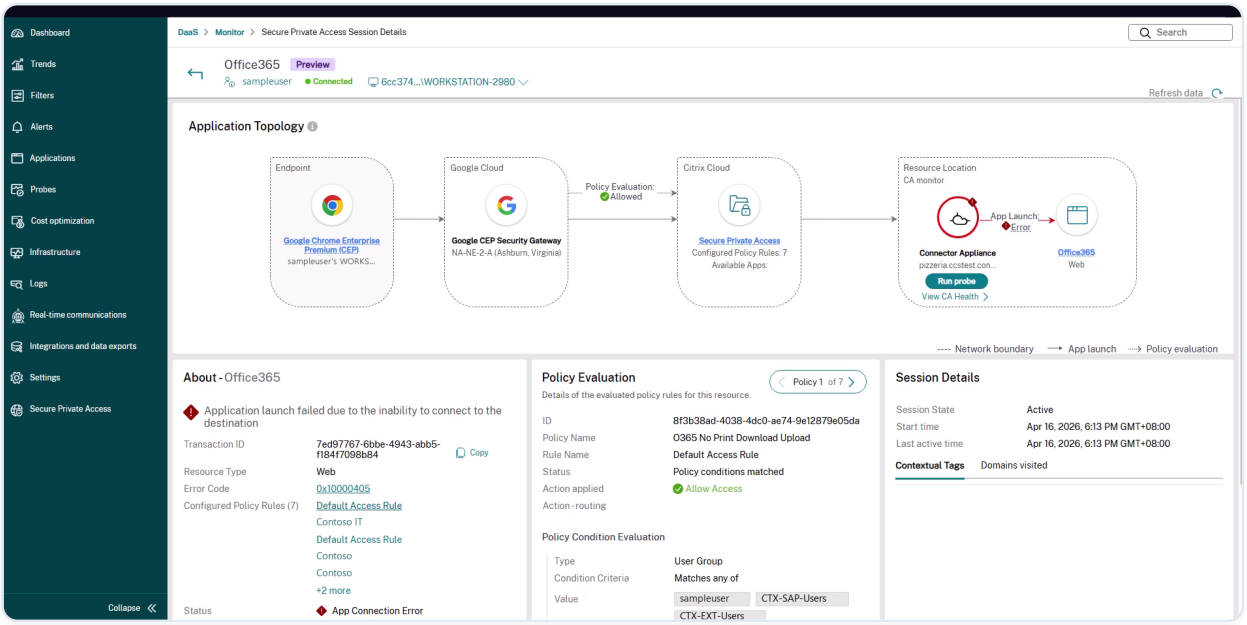
© 1997–2026 Citrix Systems, Inc. All rights reserved.

and the backend application as an **App Launch Error**, and the **About** pane shows *Application launch failed due to the inability to connect to the destination*.

1. Open the **Secure Private Access Session Details** page for the affected session. A typical path is to search for the user, open the **Activity Manager**, select the **Launched Apps (Sessions)** tab, and then click the application that reports an **Error (App Connection)** status. For more information about navigating to a session, see Monitor and troubleshoot Secure Private Access.

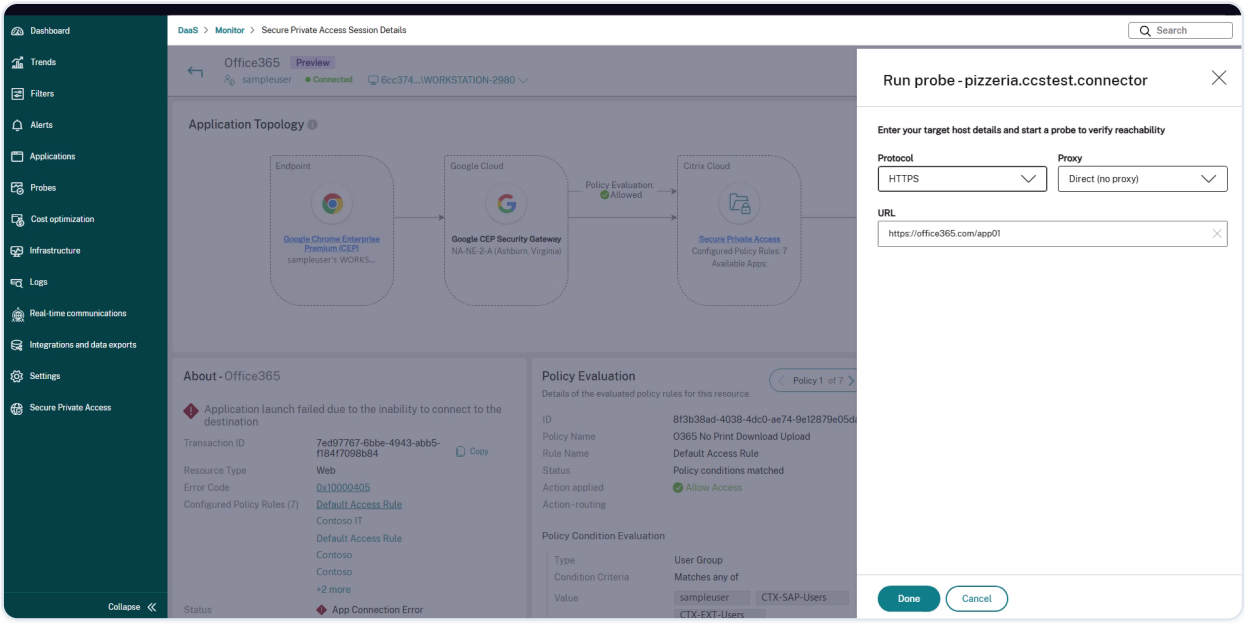


2. In the **Application Topology**, locate the **Connector Appliance** node in the **Resource Location**. When the launch failed at this hop, the node shows a **Run probe** button (and a **View CA Health** link).

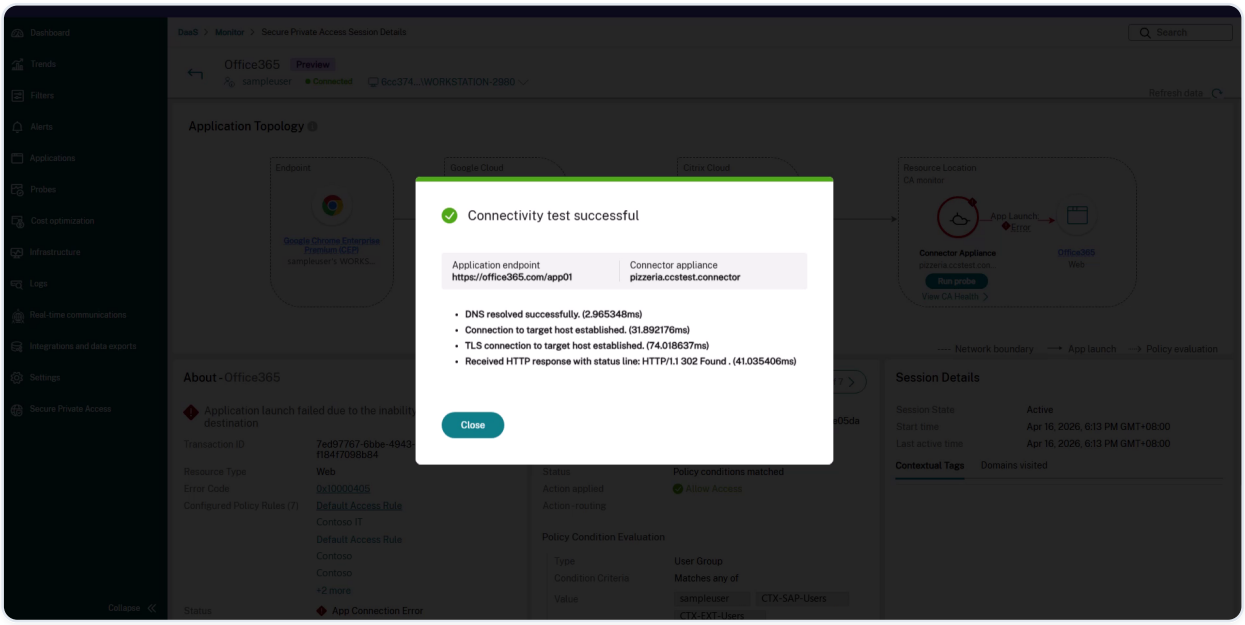


© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click **Run probe**. The **Run probe** panel opens with the **Protocol** and the application **URL** prefilled from the failed launch. Adjust the details if needed.



4. Click **Done** to start the probe, and then review the result when it finishes.



Running the probe confirms whether the selected Connector Appliance can reach the application endpoint. If the probe succeeds while the app still fails to launch, you can rule out Connector-Appliance-to-backend reachability and focus your investigation elsewhere. If the probe fails, the result shows the stage that failed, which points you to the underlying network or backend issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

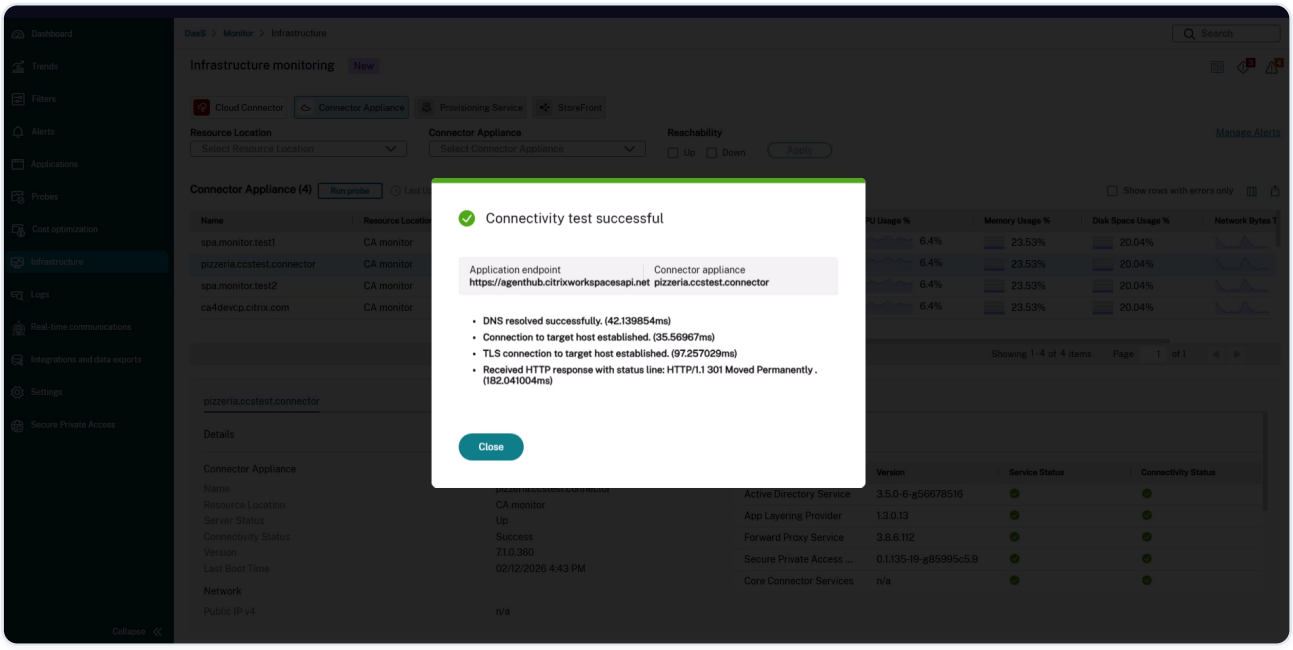
Understand the probe results

After the probe completes, Monitor shows the result for each connection stage along with the time taken. The dialog also shows the **Application endpoint** that was tested and the **Connector Appliance** that ran the probe.

Successful probe

If every stage succeeds, the dialog shows **Connectivity test successful** and lists each completed stage—for example:

- DNS resolved successfully.
- Connection to target host established.
- TLS connection to target host established.
- Received HTTP response with status line: `HTTP/1.1 301 Moved Permanently`.



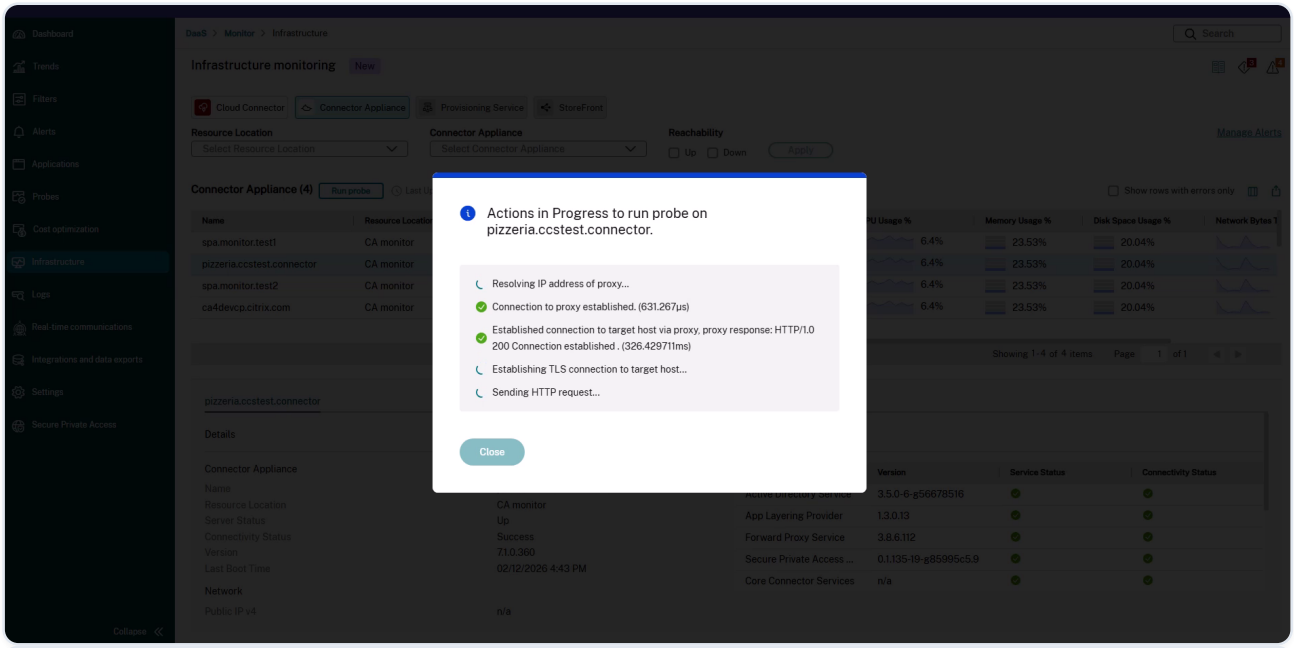
NOTE:

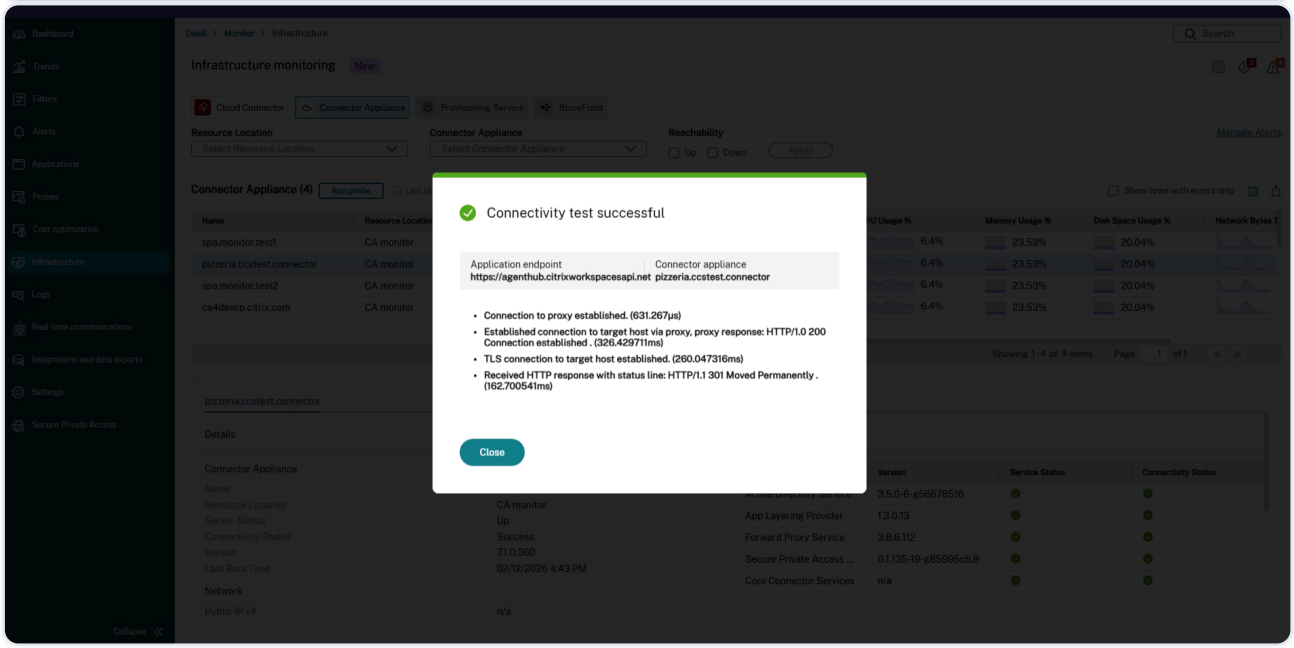
The stages shown depend on the protocol. For example, the TLS stage appears only for **SSL/TLS** and **HTTPS** probes, and the HTTP request or response stage appears only for **HTTP** and **HTTPS** probes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Probe through a proxy

When you run the probe through a proxy, the result includes the proxy connection stages before the target host stages—for example, *Connection to proxy established* and *Established connection to target host via proxy*.





Failed probe

If a stage fails, the result identifies the stage that failed and shows the associated error detail (for example, a TCP connection error such as *Connection refused*). Because the probe runs from the selected Connector Appliance, the failed stage tells you where the path breaks:

- **DNS resolution fails** – The Connector Appliance can't resolve the host name. Check DNS configuration and the host name or URL you entered.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **TCP connection fails** – The host is unreachable or the port is closed or blocked. Check the target host, port, firewall rules, and that the backend service is running.
- **TLS handshake fails** – The TCP connection succeeds but the TLS negotiation fails. Check the certificate, the TLS version, and the SNI or host name.
- **HTTP request fails** – The connection succeeds but the application returns an error or doesn't respond. Check the application and the URL path.

Considerations

- A probe is an on-demand, point-in-time connectivity test. It does not provide continuous monitoring.
- The probe runs from the data path of the selected Connector Appliance, so the result reflects that Connector Appliance's view of the network.
- A probe is expected to complete within about two minutes.
- Collecting a packet trace from the Connector Appliance is not supported from Monitor. If a packet trace is required, the network administrator must collect it from the Connector Appliance console.
- The **Connection Latency** value on the Connector Appliance to backend application hop in the Application Topology is a passive, periodic measurement (P90 over the past hour). Use a probe when you need an on-demand, point-in-time reachability test for that hop. For more information, see Connector Appliance to backend application latency.

Data granularity and retention

Aggregation of data values

The Monitor Service collects various data, including user session usage, user logon performance details, session load balancing details, and connection and machine failure information. Data is aggregated differently depending on its category. Understanding the aggregation of data values presented using the OData Method APIs is critical to interpreting the data. For example:

- Connected Sessions and Machine Failures occur over a period. Therefore, they are exposed as maximums over a time period.
- Logon Duration is a measure of the length of time, therefore is exposed as an average over a time period.
- Logon Count and Connection Failures are counts of occurrences over a period, therefore are exposed as sums over a time period.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Concurrent data evaluation

Your sessions must be overlapping to be considered concurrent. However, when the time interval is 1 minute, all sessions in that minute (whether they overlap) are considered concurrent. The size of the interval is so small that the performance overhead involved in calculating the precision is not worth the value added. If the sessions occur in the same hour, but not in the same minute, they are not considered to overlap.

Correlation of summary tables with raw data

The data model represents metrics in two different ways:

- The summary tables represent aggregate views of the metrics in per minute, hour, and day time granularities.
- The raw data represents individual events or current state tracked in the session, connection, application, and other objects.

When attempting to correlate data across API calls or within the data model itself, it is important to understand the following concepts and limitations:

- **No summary data for partial intervals.** Metrics summaries are designed to meet the needs of historical trends over long periods. These metrics are aggregated into the summary table for complete intervals. There is no summary data for a partial interval at the beginning (oldest available data) of the data collection nor at the end. When viewing aggregations of a day (Interval=1440), this means that the first and most recent incomplete days have no data. Although raw data might exist for those partial intervals, it is never summarized. Pull the min and max SummaryDate from a particular summary table to determine the earliest and latest aggregate interval for a particular data granularity. The SummaryDate column represents the start of the interval. The Granularity column represents the length of the interval for the aggregate data.
- **Correlating by time.** Metrics are aggregated into the summary table for complete intervals as described in the preceding section. They can be used for historical trends, but raw events might be more current in the state than what has been summarized for trend analysis. Any time-based comparison of summary to raw data must take into account that there is no summary data for partial intervals that might occur or for the beginning and ending of the time period.
- **Missed and latent events.** Metrics that are aggregated into the summary table might be slightly inaccurate if events are missed or latent to the aggregation period. Although the Monitor Service attempts to maintain an accurate current state, it does not go back in time to recompute aggregation in the summary tables for missed or latent events.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Connection High Availability.** During connection HA, there are gaps in the summary data counts of current connections, but the session instances are still running in the raw data.
- **Data retention periods.** Data in the summary tables is retained on a different grooming schedule from the schedule for raw event data. Data might be missing because it has been groomed away from summary or raw tables. Retention periods might also differ for different granularities of summary data. Lower granularity data (minutes) is groomed more quickly than higher granularity data (days). If data is missing from one granularity due to grooming, it might be found in a higher granularity. Since the API calls only return the specific granularity requested, receiving no data for one granularity does not mean that the data doesn't exist for a higher granularity for the same time period.
- **Time zones.** Metrics are stored with UTC time stamps. Summary tables are aggregated on hourly time zone boundaries. For time zones that don't fall on hourly boundaries, there might be some discrepancy as to where data is aggregated.

Granularity and retention

The granularity of aggregated data retrieved by Monitor is a function of the time (T) span requested. The rules are as follows:

- 0 \< T \<= 30 days use per-hour granularity
- T \> 31 days use per-day granularity

Requested data that does not come from aggregated data comes from the raw Session and Connection information. This data tends to grow fast, and therefore has its own grooming setting. Grooming ensures that only relevant data is kept long term. This ensures better performance while maintaining the granularity required for reporting.

#	SETTING NAME	SCHEMA TABLE IMPACTED	TABLES AND CHART IMPACTED IN MONITOR PAGES	RETENTION DAYS FOR PREMIUM	RETENTION DAYS FOR ADVANCED
1	GroomSessionsRetentionDays	MonitorData.Session and Monitordata.	This setting impacts session details, Logon Duration by	90	31

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING NAME	SCHEMA TABLE IMPACTED	TABLES AND CHART IMPACTED IN MONITOR PAGES	RETENTION DAYS FOR PREMIUM	RETENTION DAYS FOR ADVANCED
		Connection tables	User Session, Application Based Usage tables on the Trends page.		
2	GroomFailuresRetentionDays	MonitorData.MachineFailureLog and MonitorData.ConnectionFailureLog	Trends page: This setting impacts charts and tables on failures tab.	90	31
3	GroomLoadIndexesRetentionDays	MonitorData.LoadIndex	This setting impacts the data displayed in the "Load Evaluator Index" tab on the Trends page.	3	3
4	GroomDeletedRetentionDays	MonitorData.Machine, MonitorData.Catalog, MonitorData.DesktopGroup, and MonitorData	Machine, Catalog, DesktopGroup, and Hypervisor entities that have a LifecycleSta	90	31

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING NAME	SCHEMA TABLE IMPACTED	TABLES AND CHART IMPACTED IN MONITOR PAGES	RETENTION DAYS FOR PREMIUM	RETENTION DAYS FOR ADVANCED
		.Hypervisor entities that have a LifecycleState of ‘Deleted’. This setting also deletes any related Session, SessionDetail, Summary, Failure, or LoadIndex records.	te of ‘Deleted’. This setting also deletes any related Session, SessionDetail, Summary, Failure, or LoadIndex records.		
5	GroomSummariesRetentionDays	MonitorData.DesktopGroupSummary, MonitorData.FailureLogSummary, and MonitorData.LoadIndexSummary	This setting impacts all chart data on the Trends page.	365	31
6	GroomMachineHotfixLogRetentionDays	MonitorData.Hotfix	This setting impacts the VDA hotfix data shown on the Machine	90	31

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING NAME	SCHEMA TABLE IMPACTED	TABLES AND CHART IMPACTED IN MONITOR PAGES	RETENTION DAYS FOR PREMIUM	RETENTION DAYS FOR ADVANCED
			Details page.		
7	GroomHourlyRetentionDays	all Summary tables	This impacts the weekly graphs shown on the Trends page.	32	31
8	GroomApplicationInstanceRetentionDays	MonitorData.ApplicationInstance	This setting impacts the chart and tables on the Capacity management tab and application usage tables on the Trends page.	90	Not applicable
9	GroomNotificationLogRetentionDays	MonitorData.NotificationLog	This setting impacts the Alerts shown on Monitor.	90	Not applicable
10	GroomResourceUsageRawDataRetentionDays	MonitorData.Resourceutilization	This setting impacts CPU and Memory charts seen in "Historical Machine	3	3

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING NAME	SCHEMA TABLE IMPACTED	TABLES AND CHART IMPACTED IN MONITOR PAGES	RETENTION DAYS FOR PREMIUM	RETENTION DAYS FOR ADVANCED
			Utilization" Machine Details page and the data calculation on Cost optimization area "Workload rightsizing tab".		
11	GroomResourceUsageHourDataRetentionDays	MonitorData.Resourceutilizationsummary	This setting impacts CPU and Memory charts seen in "Historical Machine Utilization" Machine Details page and the data calculation on Cost optimization area "Workload rightsizing tab".	30	30
12	GroomResourceUsageDayDataRetentionDays	MonitorData.Resourceutilizationsummary	This setting impacts the CPU and Memory chart seen	365	31

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING NAME	SCHEMA TABLE IMPACTED	TABLES AND CHART IMPACTED IN MONITOR PAGES	RETENTION DAYS FOR PREMIUM	RETENTION DAYS FOR ADVANCED
			on Machine "Resource utilization" on Trends page and "Machine utilization" page for specific machine.		
13	GroomProcessUsageRawDataRetentionDays	MonitorData.ProcessUtilization	This setting impacts the resource trend per process information shown on machine historical usage page.	1	1
14	GroomProcessUsageHourDataRetentionDays	MonitorData.ProcessUtilizationHourSummary	This setting impacts the CPU and Memory usage trend per process shown on the machine historical usage page.	7	7
15	GroomProcessUsageD	MonitorData.ProcessUtili	This setting impacts the CPU and	30	30

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING NAME	SCHEMA TABLE IMPACTED	TABLES AND CHART IMPACTED IN MONITOR PAGES	RETENTION DAYS FOR PREMIUM	RETENTION DAYS FOR ADVANCED
	ayDataRetentionDays	zationDaySummary	Memory usage trend per process shown on the machine historical usage page.		
16	GroomSessionMetricsDataRetentionDays	MonitorData.Sessionmetrics	This setting impacts all the charts seen on the "Session Performance" tab of the user details page.	1	1
17	GroomMachineMetricDataRetentionDays	MonitorData.Machinemetrics	This setting impacts the chart and table on the "Resource Utilization" tab on the Trends page.	3	3
18	GroomMachineMetricDaySummaryDataRetentionDays	MonitorData.MachineMetricDaySummary	This setting impacts the chart and table on the "Resource Utilization" tab on the	365	31

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	SETTING NAME	SCHEMA TABLE IMPACTED	TABLES AND CHART IMPACTED IN MONITOR PAGES	RETENTION DAYS FOR PREMIUM	RETENTION DAYS FOR ADVANCED
			Trends page.		
19	GroomApplicationErrorsRetentionDays	MonitorData.ApplicationError	This setting impacts error details shown in the "Application Errors" column on the Applications page.	1	1
20	GroomApplicationFaultsRetentionDays	MonitorData.Applicationfailure	This setting impacts the "Application Faults" column on the Applications page.	1	1

CAUTION:

You cannot modify the values on the Monitor Service database.

Retaining data for long periods has the following implications on table sizes:

- **Hourly data.** If hourly data is allowed to stay in the database for up to two years, a site of 1000 delivery groups can cause the database to grow as follows:

  1000 delivery groups x 24 hours/day x 365 days/year x 2 years = 17,520,000 rows of data. The performance impact of such a large amount of data in the aggregation tables is significant.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Given that the dashboard data is drawn from this table, the requirements on the database server might be large. Excessively large amounts of data can have a dramatic impact on performance.

- **Session and event data.** This is the data that is collected every time a session is started and a connection/reconnection is made. For a large site (100 K users), this data grows fast. For example, two years' worth of these tables would gather more than a TB of data, requiring a high-end enterprise-level database.

Session launch diagnostics

NOTE:

Session launch diagnostics is currently under preview.

Session launches involve multiple Citrix components. To diagnose session launch failures, use Citrix Monitor (that is, Citrix Director service) to narrow down to the exact component and stage where the problem occurred. Apply the recommended actions to resolve the issue. Citrix Workspace™ app generates a 32-digit (8-4-4-4-12) Transaction ID which can be used in diagnosing session launch failures.

NOTE:

This feature is available only for cloud customers in the US, AP-S, and EU regions. It is not available in Japan and Government regions.

Prerequisites

If you are using Citrix DaaS™, onboarding is automatic. Cloud customers using on-premises StoreFront must ensure that a supported StoreFront version is onboarded.

- If you are using Citrix Analytics for Performance, see Data sources for the steps to onboard on-premises StoreFront.
- If you are not using Citrix Analytics for Performance™:

  a. Go to `https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Click **Connect to StoreFront deployment**, enter the details, and download the configuration file. For more information, see Onboarding on-premises sites using StoreFront.

> **NOTE:**
>
> Administrators with Cloud Administrator roles are permitted to onboard StoreFront™ deployments, while administrators with Full Monitor Administrator roles can only view the StoreFront deployments.

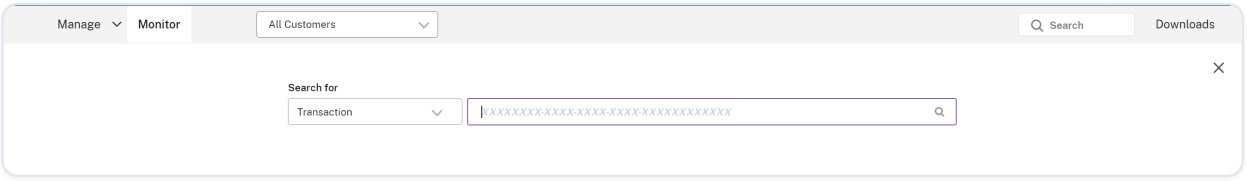
Minimum supported versions of other components are as follows:

- Citrix Workspace app for Windows 2109
- Citrix Workspace app for Mac 2112
- Citrix Workspace app for Linux 2112
- Citrix Workspace app for HTML5 2110
- Citrix Workspace app for Chrome 2110
- Citrix Workspace app for Android 2110
- VDA version Citrix Virtual Apps and Desktops™ 2112
- Citrix StoreFront 1912 LTSR CU4

Steps to diagnose session launch failure

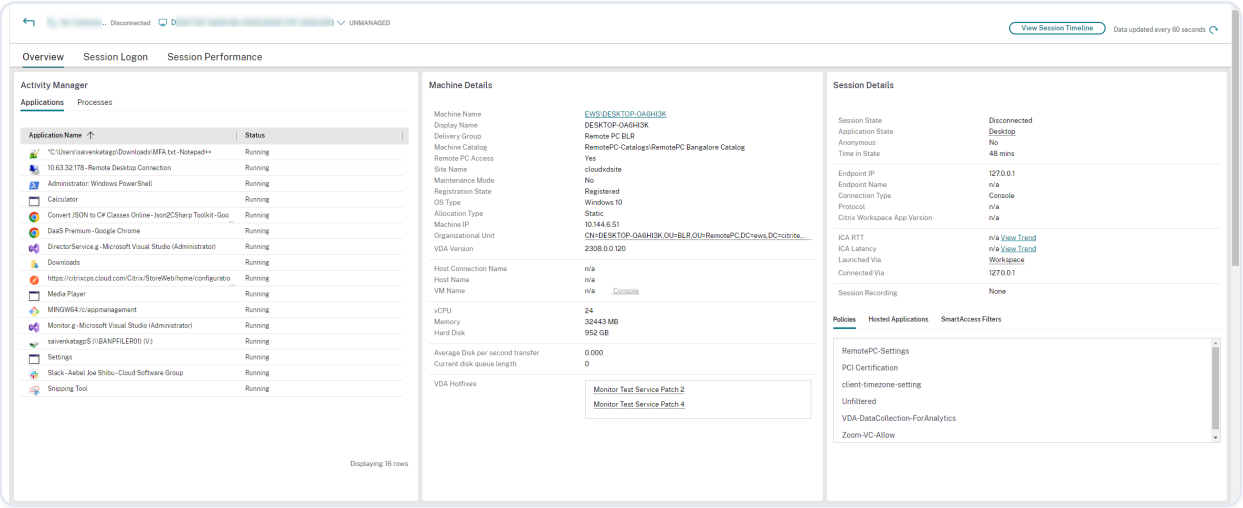
1. Copy Transaction ID of the failed session launch from Citrix Workspace app.

2. In the Monitor UI, search for the 32-digit transaction ID and click **Details**.

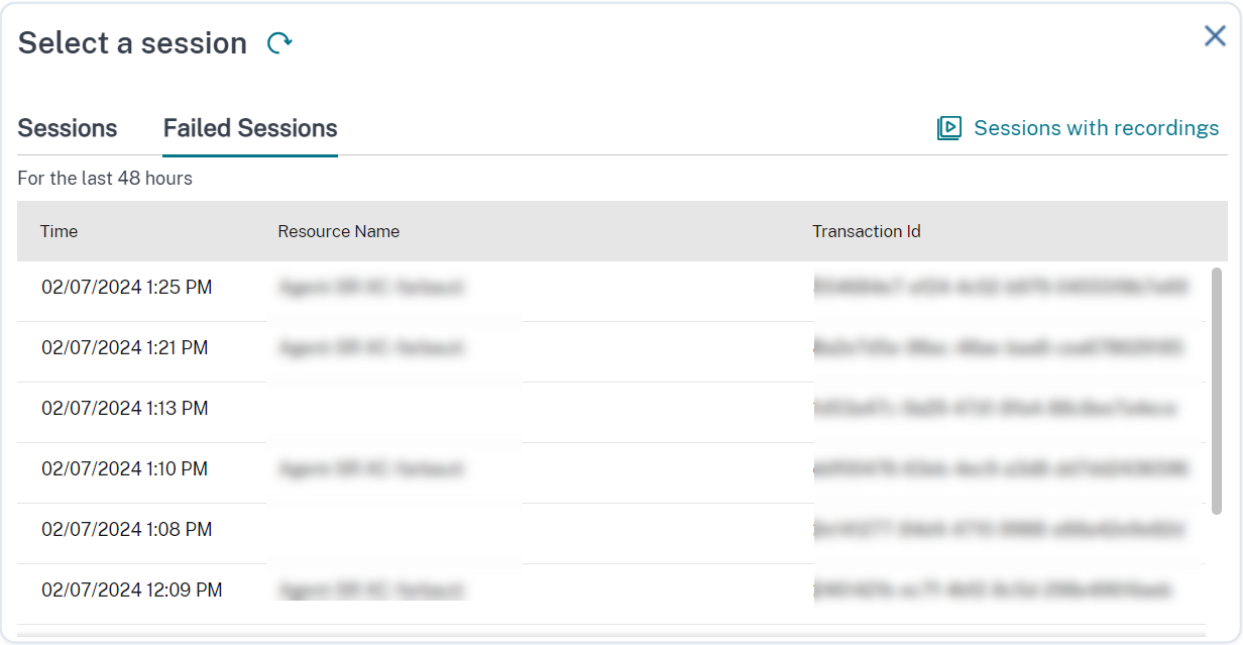


3. If Transaction ID is not available, search using the user name. The Activity Manager of the user is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click the session selector. Go to the **Failed Sessions** tab. A list of sessions that have failed during the last 48 hours is displayed. Click the selected session.



5. Citrix Monitor displays components, error details and transaction log details regarding the transaction.

The preceding screen shows the following sections:

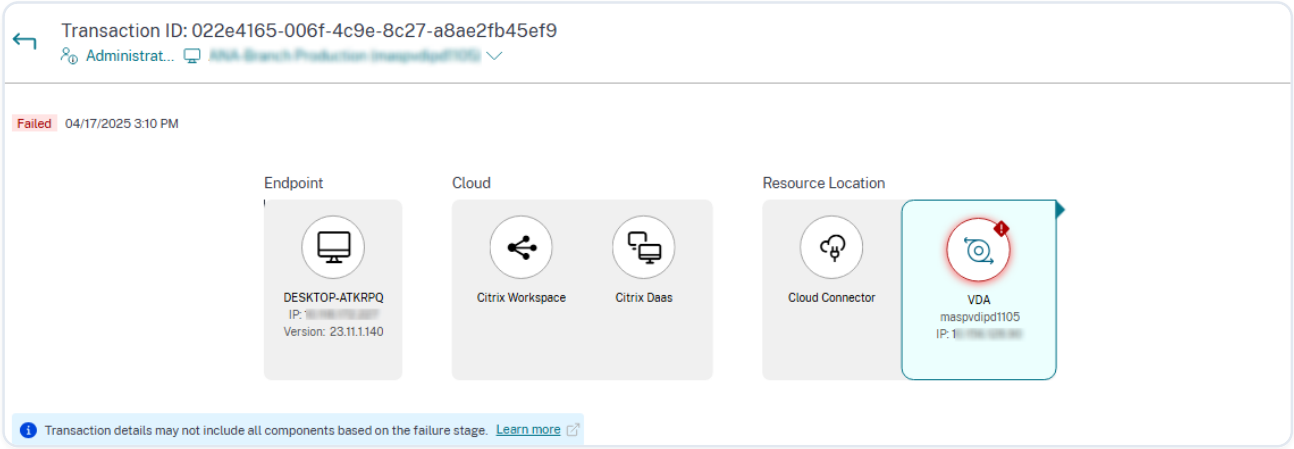
- Components
- Error Details
- Transaction Logs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Components

Depending on the session launch scenario and the failure stage, the components involved in a session are any of the following:

- Endpoint
- Citrix® StoreFront Cloud
- Citrix DaaS
- Cloud Connector
- Gateway Service
- VDA
- Citrix StoreFront



The components where the failure occurs are highlighted in the preceding image.

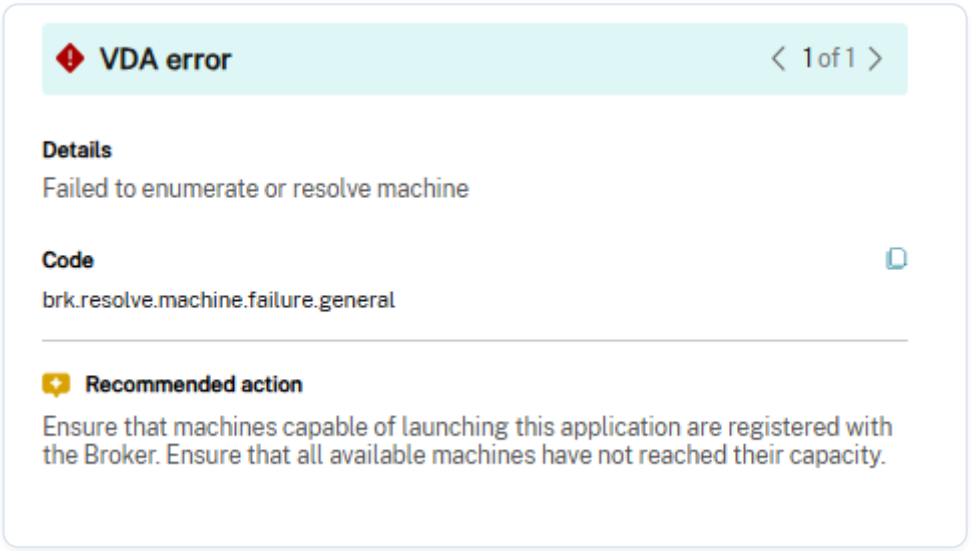
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- Transaction components are determined by the received session launch events. If a failure occurs early in the process, or the events are not received, some components may not be displayed. For example, if the error occurred in communication between the Citrix Workspace app and Citrix® StoreFront Cloud, the components would only be Endpoint and Citrix® StoreFront Cloud.
- In certain edge cases, a transaction may be considered failed, but no error is reported provided no failure events are received.
- Client-side error codes and diagnostic information are available only when Citrix StoreFront is onboarded and sending data. For more information about onboarding StoreFront, see Prerequisites. This is one reason why no error is reported for a failure session.

Error details

Error details highlight what problem occurred in a given component. Error description, error code and recommended action is displayed.



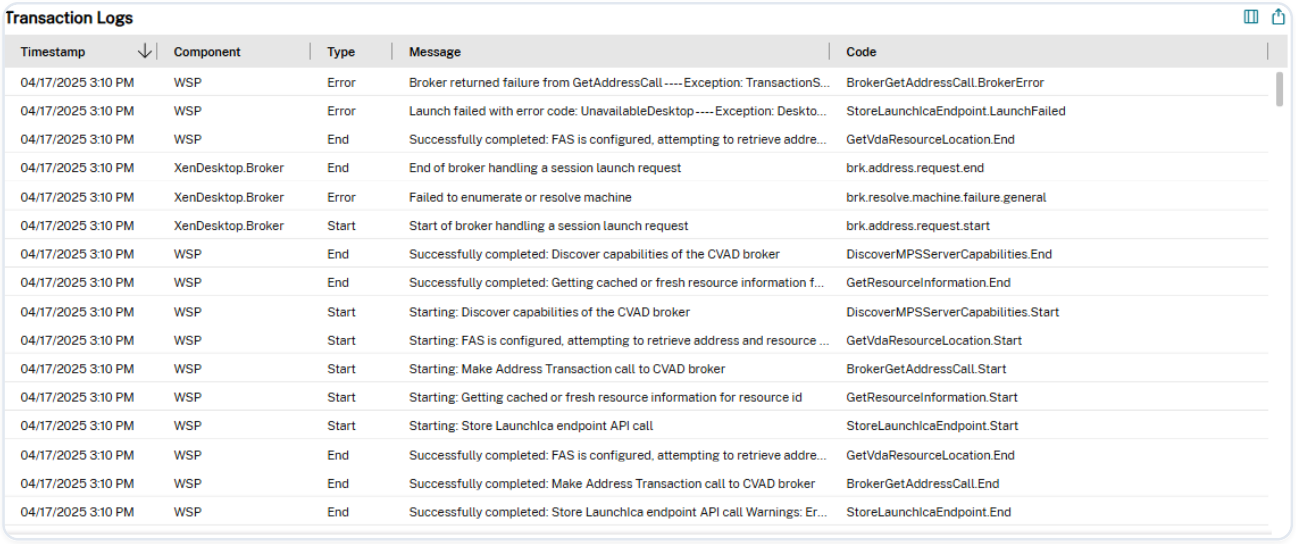
NOTE:

This section displays only the root cause of errors, not all individual errors from the raw events. For individual logs, see the Transaction logs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Transaction Logs

Transaction Logs provides the raw session launch events giving an end to end trace across components involved in the connection.



Transaction Logs

Timestamp	Component	Type	Message	Code
04/17/2025 3:10 PM	WSP	Error	Broker returned failure from GetAddressCall ---- Exception: TransactionS...	BrokerGetAddressCall.BrokerError
04/17/2025 3:10 PM	WSP	Error	Launch failed with error code: UnavailableDesktop ---- Exception: Deskto...	StoreLaunchIcaEndpoint.LaunchFailed
04/17/2025 3:10 PM	WSP	End	Successfully completed: FAS is configured, attempting to retrieve addre...	GetVdaResourceLocation.End
04/17/2025 3:10 PM	XenDesktop.Broker	End	End of broker handling a session launch request	brk.address.request.end
04/17/2025 3:10 PM	XenDesktop.Broker	Error	Failed to enumerate or resolve machine	brk.resolve.machine.failure.general
04/17/2025 3:10 PM	XenDesktop.Broker	Start	Start of broker handling a session launch request	brk.address.request.start
04/17/2025 3:10 PM	WSP	End	Successfully completed: Discover capabilities of the CVAD broker	DiscoverMPSServerCapabilities.End
04/17/2025 3:10 PM	WSP	End	Successfully completed: Getting cached or fresh resource information f...	GetResourceInformation.End
04/17/2025 3:10 PM	WSP	Start	Starting: Discover capabilities of the CVAD broker	DiscoverMPSServerCapabilities.Start
04/17/2025 3:10 PM	WSP	Start	Starting: FAS is configured, attempting to retrieve address and resource ...	GetVdaResourceLocation.Start
04/17/2025 3:10 PM	WSP	Start	Starting: Make Address Transaction call to CVAD broker	BrokerGetAddressCall.Start
04/17/2025 3:10 PM	WSP	Start	Starting: Getting cached or fresh resource information for resource id	GetResourceInformation.Start
04/17/2025 3:10 PM	WSP	Start	Starting: Store LaunchIca endpoint API call	StoreLaunchIcaEndpoint.Start
04/17/2025 3:10 PM	WSP	End	Successfully completed: FAS is configured, attempting to retrieve addre...	GetVdaResourceLocation.End
04/17/2025 3:10 PM	WSP	End	Successfully completed: Make Address Transaction call to CVAD broker	BrokerGetAddressCall.End
04/17/2025 3:10 PM	WSP	End	Successfully completed: Store LaunchIca endpoint API call Warnings: Er...	StoreLaunchIcaEndpoint.End

Error code

Broker agent

bka.prepare.session.failure.validation

- Description: Failed to validate the prepare session request.
- Recommended Action: Retry action. If failure repeats, check that the connectors are in a healthy state.

bka.prepare.session.failure.rejected

- Description: VDA cannot accept the launch request.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

bka.hdx.prepare.failure.general

- Description: HDX™ prepares failure.
- Recommended Action: Restart the VDA.

bka.hdx.validate.failure.ticket_not_found

- Description: Referenced ticket or launch not in launch cache.
- Recommended Action: Ensure that VDA can communicate with the connector.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

bka.ticketing.validate.failure.unlicensed

- Description: Cannot verify license for launch.
- Recommended Action: Contact Citrix Support.

bka.ticketing.validate.failure.general

- Description: Generic failure while validating a ticket.
- Recommended Action: Gather logs on the VDA and Contact Citrix Support.

bka.set.configuration.failure.policy

- Description: An error occurred during setting policies.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

bka.set.configuration.failure

- Description: An error occurred during setting configuration.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

Broker

brk.validate.credentials.failure.invalid

- Description: Failed to validate credentials due to some issue. The reason can be expanded in the message parameter.
- Recommended Action: Retry action. If failure repeats, check that the connectors are in a healthy state.

brk.resolve.machine.failure.general

- Description: Failed to enumerate or resolve worker. The reason can be expanded in the message parameter.
- Recommended Action: Ensure that machines capable of launching this application are registered with the Broker. Ensure that all available machines have not reached their capacity.

brk.license.check.failure.constraints

- Description: Licensing constraints failed session launch.
- Recommended Action: Ensure that there are licenses available for this type of application or desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

brk.resolve.machine.failure.timeout

- Description: Broker timed out while contacting the database.
- Recommended Action: Problems communicating with the site database. Contact Citrix support.

brk.poweron.forlaunch.queued.failure.general

- Description: Queueing power action failed.
- Recommended Action: Problems communicating with the site database. Contact Citrix support.

brk.set.configuration.failure.general

- Description: Unspecified error while setting configuration on target VDA.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

brk.prepare.session.failure.host_unreachable

- Description: Failed to communicate with the VDA.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

brk.prepare.session.failure.general

- Description: Failed to prepare session on VDA, UnsupportedClientType, or ConnectionRefused errors.
- Recommended Action: Restart Citrix Delivery Agent service on VDA or restart VDA.

brk.validate.ticket.failure.license

- Description: Failed to retrieve a valid license for this session.
- Recommended Action: Check the health status of the site and ensure all connectors and the Citrix DDC are operational.

brk.validate.ticket.failure.general

- Description: Invalid ticketing call.
- Recommended Action: Contact Citrix support.

brk.reverse.prepare.failure.general

- Description: Generic failure during session launch.
- Recommended Action: Check the health status of the site and ensure all connectors and the Citrix DDC are operational.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

brk.reverse.prepare.failure.lease_revoked

- Description: Lease for this session was revoked.
- Recommended Action: Retry action, if failure repeats, check that the connectors are in a healthy state.

brk.reverse.prepare.failure.resource_unavailable

- Description: The resource is already in use or is temporarily unavailable.
- Recommended Action: Retry action, if failure repeats, check that the connectors are in a healthy state.

brk.reverse.prepare.failure.app_protection

- Description: App Protection is missing and is required for this session.
- Recommended Action: Ensure that app protection is enabled on this VDA or remove the App Protection requirement from the application.

HDX VDA Linux

VDA_LINUX_ERR_RECONNECT_PRE_LOGOFF

- Description: Reconnect to a session in pre-logoff state is not allowed.
- Recommended action: Retry to launch the later, this gives time to let the session logoff.

VDA_LINUX_ERR_RECONNECT_NO_SESSION

- Description: Reconnect to a non-exiting session.
- Recommended action: Retry to launch latter. If still fail, contact Citrix support.

VDA_LINUX_ERR_SAME_KEY

- Description: Prepare for a connection, but there is an existing session with the same session key.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_GET_FQDN

- Description: Failed to get the FQDN of this VDA.
- Recommended action: Verify that the DNS configuration on the VDA is correct

VDA_LINUX_ERR_NO_CGP_LISTENER

- Description: There is no a CGP listener running.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended action: Verify **Session reliability connections** policy is enabled. Verify that the CGP listener is listening on expected port in VDA (default port is 2598, can be changed via **Session reliability port number** policy).

VDA_LINUX_ERR_DTLS_CONNECT

- Description: Failed to establish a DTLS connection to Gateway service.
- Recommended action: Verify that the Gateway service FQDN is reachable from VDA. Verify path `/var/xdl/keystore/cacerts` exists in VDA. Remove `/var/xdl/keystore` and run `/var/xdl/split_ca_bundle.sh` to regenerate CA certificates. Verify that the Gateway service FQDN is trusted by VDA.

VDA_LINUX_ERR_ACCEPT_EDT_CONNECT

- Description: Failed to accept EDT handshake from client.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_TCP_CONNECT

- Description: Failed to establish a TCP connection to Gateway service.
- Recommended action: Verify that the Gateway service FQDN is reachable from VDA.

VDA_LINUX_ERR_TLS_CONNECT

- Description: Failed to establish a TLS handshake to Gateway service.
- Recommended action: Verify path `/var/xdl/keystore/cacerts` exists in VDA. Remove `/var/xdl/keystore` and run `/var/xdl/split_ca_bundle.sh` to regenerate CA certificates. Verify that Gateway service FQDN is trusted.

VDA_LINUX_ERR_RDVZ_HANDSHAKE

- Description: Failed to establish a rendezvous handshake to Gateway service.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_ACCEPT_ICA_CONNECT

- Description: Failed to accept an ICA® connection.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_RECONNECT_TO_ANON_SESSION_NOT_ALLOWED

- Description: Reconnect to an anonymous session is not allowed.
- Recommended action: Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA_LINUX_ERR_CONN_NOT_ALLOWED

- Description: Connection is not allowed.
- Recommended action: If the result code is 3, verify that the license is not expired, otherwise, retry launch later. If you are unable to resolve, contact Citrix support.

VDA_LINUX_ERR_CONN_GENERAL

- Description: Failed to validate connection.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_USER_CANCELLED_LOGIN

- Description: End user canceled logon.
- Recommended action: This error is expected, when SSO is disabled, and the end user clicks at the 'Cancel' button in the logon box, otherwise, Contact Citrix support.

VDA_LINUX_ERR_GET_TARGET

- Description: Failed to get the target session.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_START_LOGON_TIMERS

- Description: Failed to start logon timers.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_SEND_CMD_TO_TARGET

- Description: Failed to send command to target session.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_POST_RECONNECT_EVENT

- Description: Failed to post a reconnect event.
- Recommended action: Contact Citrix support.

VDA_LINUX_ERR_RECONNECT_TIMEOUT

- Description: Reconnect to user session timeout.
- Recommended action: Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX VDA Windows

RENDEZVOUS_CONNECT_FAILED_TCP

- Description: Outbound rendezvous connection attempt from VDA to Citrix Gateway rendezvous point over TCP failed.
- Recommended action:
  - Review rendezvous and UDP/DTLS network configuration on VDA.
  - Raise support ticket if all the above seems appropriate. Share AO and CDF traces from VDA and network packet capture from gateway/VDA (if possible).

RENDEZVOUS_CONNECT_FAILED_EDT

- Description: Outbound rendezvous connection attempt from VDA to Citrix Gateway rendezvous point over EDT failed.
- Recommended action:
  - Review rendezvous and UDP/DTLS network configuration on VDA and CGS.
  - Raise support ticket if all the above seems appropriate. Share AO and CDF traces from VDA and network packet capture from gateway/VDA (if possible).

RENDEZVOUS_CONNECT_FAILED_PROXY

- Description: Outbound rendezvous connection attempt from VDA to Citrix Gateway rendezvous point via proxy failed.
- Recommended action:
  - Review rendezvous proxy configuration in consultation with Citrix documentation.
  - Raise support ticket if all the above seems appropriate. Share AO and CDF traces from VDA and network packet capture from gateway/VDA (if possible).

RENDEZVOUS_CONNECT_FAILED_DTLS

- Description: Outbound rendezvous connection attempt from VDA to Citrix Gateway rendezvous point failed due to DTLS handshake failure.
- Recommended action:
  - Review rendezvous and UDP/DTLS network configuration on VDA.
  - Review rendezvous and cryptographic requirements based on Citrix documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Raise support ticket if all the above seems appropriate. Share AO and CDF traces from VDA and network packet capture from gateway/VDA (if possible).

RENDEZVOUS_CONNECT_FAILED_TLS

- Description: Outbound rendezvous connection attempt from VDA to Citrix Gateway rendezvous point failed due to TLS handshake failure.
- Recommended action:
  - Review rendezvous and TCP/DTLS network configuration on VDA.
  - Review rendezvous and cryptographic requirements based on Citrix documentation.
  - Raise support ticket if all the above seems appropriate. Share AO and CDF traces from VDA and network packet capture from gateway/VDA (if possible).

RENDEZVOUS_CONNECT_FAILED_CGP

- Description: An outbound Rendezvous transport connection attempt failed due to a CGP configuration issue.
- Recommended action: Check that CGP (Session Reliability) is enabled and CGP ports are being listened on, contact Citrix support.

CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT

- Description: VDA enters Session Reliability (SR) when ICA session experiences a network disruption causing the interruption in packet flow. If this network issue is not resolved within a specified period (default set to 180 second, refer Citrix policy documentation) a timeout might occur indicated by CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT event.
- Recommended action:
  - If the ICA session does not reconnect within the timeout period, end-user can review network connectivity on the client, e.g. network and internet setting on Windows taskbar.
  - While the ICA session is in Session Reliability mode, try opening an internet resource in a web browser on client to ensure internet access works as expected.
  - If the website loads but the ICA session fails to reconnect, further debugging is required. Raise support ticket with AO logs and preferably CDF traces from VDA and Client.

CGP_SR_SUSPEND_RESUME_FAILED

- Description: VDA enters Session Reliability (SR) when ICA session experiences a network disruption causing the interruption in packet flow. CGP_SR_SUSPEND_RESUME_FAILED

© 1997–2026 Citrix Systems, Inc. All rights reserved.

event indicates there was a failure processing the suspend or resume request other than timeout.

- Recommended action: Raise support ticket with AO logs and preferably CDF traces, network topology especially usage of branch repeaters.

PREPARE_RECONNECT_REJECTED

- Description: VDA rejected a reconnect request from an incoming ICA connection due to an invalid session key.
- Recommended action:
  - Review the event logs on VDA for listener creation errors.
  - Alternatively check if the listeners are active. On RDS machines, 'netstat -a' can list the ports and corresponding owners. Review if any application is already using ports designated for ICA.
  - Raise a support ticket with Citrix and include AO logs and preferably CDF traces for all modules on client and VDA

Error: PREPARE_REJECTED

- Description: VDA rejected a connect request from an incoming ICA connection due to an invalid session key.
- Recommended action: Check VDA configuration, contact Citrix support.

PREPARE_LISTENING_FAILED

- Description: VDA failed to start listeners for the incoming ICA connection.
- Recommended action: Check network configuration, verify that listener ports are not in use by other applications, contact Citrix support.

RENDEZVOUSCONNECTIONREQ_FAILED

- Description: VDA failed to notify the ICA Stack to start an outbound Rendezvous connection.
- Recommended action: Check rendezvous configuration, check rendezvous proxy configuration, check CGP (Session Reliability) configuration, contact Citrix support.

RENDEZVOUSCONNECTIONREQ_FAILED_PROXYCONFIG

- Description: VDA failed to request the ICA Stack to start an outbound Rendezvous connection due to a proxy configuration error.
- Recommended action: Check rendezvous proxy configuration, contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ESTABLISH_SESSION_FAILED

- Description: VDA failed to create a session for the incoming ICA connection or failed to connect to an existing session.
- Recommended action: Raise support ticket with AO logs and preferably CDF traces for all modules on client and VDA.

ICA_ESTABLISH_FAILED

- Description: A transport connection is received but the connection establishment fails during handshake.
- Recommended action:
  - Review port scanning software that scan ICA ports like 1494, 2598 which may have listeners always enabled to receive any connection request, therefore may spit out these messages as failed attempts. Or filter the errors in splunk that have no pre-launch sequence required for ICA session.
  - Raise support ticket with AO logs and preferably CDF traces, Wireshark captures (if possible) from VDA and Client for other failure.

VALIDATE_FAILED

- Description: Broker failed to validate an incoming ICA connection request from the VDA.
- Recommended action: Raise support ticket with AO logs and preferably CDF traces for all modules on client and VDA.

VALIDATE_TICKETING_FAILED

- Description: Broker failed to validate an incoming ICA connection request from the VDA because of a ticketing issue.
- Recommended action: Raise support ticket with AO logs and preferably CDF traces for all modules on client and VDA.

PREPARE_FAILED

- Description: Generally means prepare for incoming ICA session failed on VDA due to some error.
- Recommended action:
  - Review the session state in Citrix Studio to confirm that sessions have been logged out and not lingering around.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Check if the listeners are started. Review event viewer on VDA for listener creation errors.
- Raise a support ticket with Citrix and include AO logs and preferably CDF traces for all modules on client and VDA

MCS

brk.poweron.forlaunch.execution.generalfailure

- Description: General errors.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.insufficientresourcefailure

- Description: A hypervisor operation cannot be completed because of insufficient resources on the hypervisor.
- Recommended action: Check the resource quota in the hypervisor. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.nosuchmanagedmachine

- Description: A machine ID does not exist.
- Recommended action: Check the machine ID in the hypervisor. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.hypervisorconnectionfailure

- Description: Unable to establish a connection to the hypervisor. For example, the hosting infrastructure address was not found.
- Recommended action: Verify that the hosting infrastructure address is correct. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.invalidcredentialsfailure

- Description: Invalid credentials.
- Recommended action: Check the credentials for the hypervisor connection. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.authorizationfailure

- Description: Insufficient privilege or credentials.
- Recommended action: Check the permission assigned to the credentials for the hypervisor connection. If you cannot find a solution, contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

brk.poweron.forlaunch.execution.sslcertauthfailure

- Description: A connection cannot be established due to an SSL authentication issue.
- Recommended action: Check the hypervisor's connection certificate. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.ratelimitedfailure

- Description: Cloud connection reports that it is rate limiting.
- Recommended action: Retry the connection later if the request is blocked by the hypervisor's rate limitation. If you cannot find a solution, contact Citrix support.

brk.poweron.forlaunch.execution.connectorconnectionfailure

- Description: Errors exist on the cloud connector. For example, a timeout occurs while waiting for the connection. Once the timeout is reached, the cloud connector is disconnected.
- Recommended action: Restart the cloud connector. If that fails contact Citrix support.

brk.poweron.forlaunch.execution.remotehclserverconnectionfailure

- Description: Errors on the HCL/remote proxy plug-in or end point were not found when setting up the connection to the plug-in.
- Recommended action: Restart the connector. If that fails, contact Citrix support.

brk.poweron.forlaunch.execution.expiredcredentialsfailure

- Description: An expired credential was provided.
- Recommended action: Refresh the expired credentials used by the hypervisor connection.

brk.poweron.forlaunch.execution.mcsmachinemanagementcustomfailure

- Description: Errors during machine creation.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.detachdiskfailed

- Description: The detach disk used by the virtual machine failed.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.createclonefailed

- Description: Create clone disk failed in hypervisor.
- Recommended action: Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

brk.poweron.forlaunch.execution.provisionedvmnotfound

- Description: The provisioned VM was not found.
- Recommended action: Remove the provisioned VM from the catalog. If that fails, contact Citrix support.

brk.poweron.forlaunch.execution.invalidvmstate

- Description: The operation cannot proceed due to an invalid VM state.
- Recommended action: Restart the VM first and retry the operation.

brk.poweron.forlaunch.execution.insufficientresources

- Description: Insufficient resources during operation.
- Recommended action: Check the resource quota used by the hypervisor.

brk.poweron.forlaunch.execution.hypervisorinmaintenancemode

- Description: The operation cannot proceed because the hypervisor is in maintenance mode.
- Recommended action: Verify if the hypervisor is in maintenance mode.

brk.poweron.forlaunch.execution.delayed

- Description: Operation is queued.
- Recommended action: Wait for the process to complete. If the operation fails, contact Citrix support.

brk.poweron.forlaunch.execution.recreatevmfailed

- Description: The recreation of the VM failed.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.unknownvirtualmachine

- Description: Unknown virtual machine.
- Recommended action: Contact Citrix support.

brk.poweron.forlaunch.execution.ratelimitexceed

- Description: The cloud connection is rate limiting.
- Recommended action: Retry the connection later if the request was blocked by the hypervisor's rate limitation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

brk.poweron.forlaunch.execution.virtualdisknotyetonstorage

- Description: The virtual disk is not stored.
- Recommended action: Retry later. If that fails, contact Citrix support.

Profile Management

xendesktop.upm.userprofile.error.failure

- Description: Citrix Profile Management failed to process the user profile. Use a temporary profile instead.
- Recommended action: This error doesn't cause a logon failure. Citrix Profile Management uses a temporary profile instead. To troubleshoot the error, check the Windows Event logs.

xendesktop.upm.userprofile.error.timeout

- Description: Citrix Profile Management failed to process the user profile within the specified time.
- Recommended action: This error doesn't cause a logon failure. Citrix Profile Management continues processing the user profile. To troubleshoot the error, check the Citrix Profile Management logs.

WEM Agent

wem.agent.userpolicy.error.failure

- Description: The Workspace Environment Management™ (WEM) agent failed to process group policies for the user. The user logon continues.
- Recommended action: The error does not cause logon failures. For more details, see the WEM product documentation and check the WEM agent service logs.

wem.agent.userpolicy.error.timeout

- Description: The Workspace Environment Management (WEM) agent failed to process group policies for the user within the specified time. The user logon continues.
- Recommended action: The error does not cause logon failures. For more details, see the WEM product documentation and check the WEM agent service logs.

Android Postlaunch

SessionManager.Launch.EngineLoadFailed

- Description: Failed to load or initialize ICA Engine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended Action: Contact Citrix support.

SessionManager.Launch.ConnectionFailed

- Description: Engine terminated before connecting.
- Recommended Action: Contact Citrix support.

SessionManager.Launch.LogonFailed

- Description: Session disconnected without completing login.
- Recommended action: Contact Citrix support.

SessionManager.LeaseResolution.Failed

- Description: Unable to attempt lease launch.
- Recommended Action: Contact Citrix support.

SessionManager.clxmtp.SoftDeny

- Description: Engine CLXMTP negotiation failed (soft deny).
- Recommended Action: Contact Citrix support.

SessionManager.clxmtp.SoftDeny_Implicit

- Description: Engine CLXMTP connection failed (implicit soft deny).
- Recommended Action: Contact Citrix support.

Transport.Connect.NoCGP_Fail

- Description: Failed to connect (CGP disabled).
- Recommended Action: Contact Citrix support.

Transport.Connect.FallbackFail

- Description: Failed to connect. Tried the ICA fallback.
- Recommended Action: Contact Citrix support.

Transport.Connect.Fail

- Description: Connection is unavailable.
- Recommended Action: Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android Prelaunch

CWA-ICADOWNLOAD_ERR_00001

- Description: Send ICA request type is incorrect.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00002

- Description: The ICA request is invalid.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00003

- Description: The store is null for the ICA request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00004

- Description: The store URL is null for the ICA request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00005

- Description: The resource parameter is null for the ICA request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00006

- Description: The resource parameter provided for the ICA request isn't a valid resource type.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00007

- Description: The resource parameter provided for the ICA request is null for the ICA launch URL.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00008

- Description: The ICA request is null with authentication manager parameters.
- Recommended Action: Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CWA-ICADOWNLOAD_ERR_00009

- Description: The ICA request body is null.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00010

- Description: Failed to create an HTTP entity from the ICA request body.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00011

- Description: Failed to download the ICA file because of an exception from creating the authentication manager request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00012

- Description: Failed to download the ICA file because of an exception from running the authentication manager request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00013

- Description: Failed to download the ICA file because of an unexpected response from the authentication manager request.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00014

- Description: Failed to download the ICA file when you copy the inputStream from the authentication manager response.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00015

- Description: Failed to parse the ICA document using the inputStream from the authentication manager response.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00016

- Description: The ICA document downloaded is null without any exception.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00017

- Description: Failed to download the ICA file because of an unsuccessful response.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00018

- Description: Resource is unavailable.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00019

- Description: The resource to launch either does not exist, not enabled, or not visible to a user.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00020

- Description: There are no more active sessions.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00021

- Description: The server does not have the required license to do the requested activity.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00022

- Description: There are no workstations available.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00023

- Description: Unable to connect to the workstation. The Server has refused the connection.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00024

- Description: The workstation is under maintenance and is unavailable for use.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00025

- Description: Can't launch the resource because of a `resourceerror` error in the ICA file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00026

- Description: Can't launch the resource because of a `generalapplauncherror` error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00027

- Description: Can't launch the resource because of an unknown error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00028

- Description: Can't launch the resource because of a rebooting error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00029

- Description: Can't launch the resource because of a resuming error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00030

- Description: Can't launch the resource because of an undefined error in the ICA file.
- Recommended Action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00031

- Description: Can't download the ICA file. However, the error code isn't found in the defined map.
- Recommended Action: Contact Citrix support.

Linux Postlaunch

SessionManager.Launch.EngineLoadFailed

- Description: Failed to load ICA engine.
- Recommended action: Contact Citrix support.

SessionManager.Launch.Failed

- Description: Failed to launch the session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended Action: Contact Citrix support.

SessionManager.Launch.ConnectionFailed

- Description: Engine terminated before connecting.
- Recommended Action: Look for other errors associated with the launch attempt.

SessionManager.Launch.LogonFailed

- Description: Session disconnected without completing login.
- Recommended Action: This error indicates login failure, possibly including a failure of the user to manually enter credentials. Investigate how the user attempted to sign into the remote VDA.

SessionManager.LeaseResolution.Failed

- Description: Unable to attempt lease launch.
- Recommended Action: Verify that the leases have been synced to the client machine, and are still valid. User can sign into their store in online mode to trigger the (re-) sync of leases. Look for errors that the Gateway or Cloud Connector components sent. These errors might indicate reasons for the failure.

Transport.Connect.NoCGP_Fail

- Description: Failed to connect (CGP disabled).
- Recommended Action: Investigate why the client isn't able to contact a VDA via TCP or EDT.

Transport.Connect.FallbackFail

- Description: Failed to connect. Tried the ICA fallback.
- Recommended Action: Investigate why the client isn't able to contact a Gateway, Connector, or VDA via either TCP or EDT.

Transport.Connect.Fail

- Description: Citrix Workspace app failed to connect to Gateway, Connector, or VDA through TCP, EDT, or UDP.
- Recommended Action: Investigate why the client isn't able to contact the Gateway, Connector, or VDA through TCP, EDT, or UDP. The firewall between the client and host might not allow the protocols(UDP/TCP) or the required ports.

SessionManager.clxmtp.SoftDeny

- Description: Engine CLXMTP negotiation failed (soft deny).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended Action: This error doesn't indicate that the launch must fail. It indicates that the engine can't succeed through a specific network path. Look for errors that the Gateway or Cloud Connector components sent. These errors might indicate reasons for the failure.

SessionManager.clxmtp.SoftDeny_Implicit

- Description: Engine CLXMTP connection failed (implicit soft deny).
- Recommended Action: This error doesn't indicate that the launch must fail. It indicates that the engine can't succeed through a specific network path. Investigate why the client can't contact a Connector or Gateway. It might be expected for that host to be inaccessible because of network topology or firewall restrictions.

Linux Prelaunch

CWA-ICADOWNLOAD_ERR_00001

- Description: Unable to connect to store because of no response from the Citrix Workspace app.
- Recommended action: Verify whether Citrix® StoreFront Cloud or Citrix® StoreFront is down. Also, verify the internet connectivity.

CWA-ICADOWNLOAD_ERR_00002

- Description: User has canceled the session launch.
- Recommended action: Relaunch the session after sometime.

CWA-ICADOWNLOAD_ERR_00003

- Description: Unable to connect to store. Verify that the server certificates are valid.
- Recommended action: Verify if server certificates are installed and active.

CWA-ICADOWNLOAD_ERR_00004

- Description: The resource to launch does not exist, not enabled, or not visible to a user.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00005

- Description: Workstations aren't available for this request.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00006

- Description: Server does not have the required license to do the requested activity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00007

- Description: Server has refused connection to workstation.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00008

- Description: The requested workstation is under maintenance and is unavailable for use.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00009

- Description: Maximum session limit is reached.
- Recommended action: Reached the maximum session limit that was configured by an admin. Restart the session.

CWA-ICADOWNLOAD_ERR_000010

- Description: General error that cannot be further specified.
- Recommended action: Contact Citrix support.

Mac Postlaunch

Desktop failed to start

- Description: "Desktop name" desktop failed to start. Transaction ID - "Transaction ID".
- Recommended action: Contact your admin with the error details.

Viewer failed to start

- Description: Viewer failed to start. Transaction ID - "Transaction ID".
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: "Desktop name" desktop is under planned maintenance. Transaction ID - "Transaction ID".
- Recommended action: Contact your admin with the error details.

Application failed to start

- Description: "App name" failed to start.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended action: Contact your admin with the error details.

Application failed to start

- Description: "App name" failed to start. Transaction ID - "Transaction ID".
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: "Desktop name" desktop failed to start.
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: "Desktop name" desktop failed to start. Transaction ID - "Transaction ID".
- Recommended action: Contact your admin with the error details.

Viewer failed to start

- Description: Viewer failed to open "Application name". Transaction ID - "Transaction ID".
- Recommended action: Contact your admin with the error details.

Viewer failed to start

- Description: Viewer failed to open desktop "Desktop name". Transaction ID - "Transaction ID".
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: "Desktop name" desktop is under planned maintenance.
- Recommended action: Contact your admin with the error details.

Desktop failed to start

- Description: "Desktop name" desktop is under planned maintenance. Transaction ID - "Transaction ID".
- Recommended action: Contact your admin with the error details.

Unable to connect to the desktop

- Description: Unable to reach "desktop name" desktop. Transaction ID - "Transaction ID". Try again later.
- Recommended action: If the problem persists, contact your admin with the error details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mac Prelaunch

CWA-ICADOWNLOAD_ERR_00001

- Description: ICA file is invalid.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00002

- Description: Launch request has timed out.
- Recommended action: Verify the internet connection or contact Citrix support.

CWA-ICADOWNLOAD_ERR_00003

- Description: Server did not respond.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00004

- Description: Resource to launch either doesn't exist, isn't enabled, or isn't visible to the user.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00005

- Description: Server isn't reachable.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00006

- Description: Error while launching the viewer.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00007

- Description: Failed to launch an Apple open event.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00008

- Description: Viewer path isn't reachable.
- Recommended action: Contact Citrix support.

CWA-ICADOWNLOAD_ERR_00009

- Description: User canceled the authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended action: Ask the user to relaunch the resource.

CWA-ICADOWNLOAD_ERR_000010

- Description: User canceled the LSI Window.
- Recommended action: Ask the user to relaunch the resource.

CWA-ICADOWNLOAD_ERR_000011

- Description: Requested Workstation is under maintenance and unavailable for use.
- Recommended action: Ask the user to try after maintenance is complete, and the workstation is available for use.

CWA-ICADOWNLOAD_ERR_000012

- Description: User login credentials must be changed.
- Recommended action: Ask user to change login credentials.

CWA-ICADOWNLOAD_ERR_000013

- Description: The session connecting the resource is no longer active.
- Recommended action: Ask the user to try again, or contact your Citrix technical support for further assistance.

CWA-ICADOWNLOAD_ERR_000014

- Description: Failed to download ICA file.
- Recommended action: Contact Citrix support.

Windows Postlaunch

SessionManager.Launch.EngineLoadFailed

- Description: The core components for establishing a connection to a remote desktop or application failed to load or initialize properly. Extra details might be provided in the error message.
- Recommended action: Citrix Workspace app isn't functioning as expected. A third-party (non-Citrix) virtual channel DLL or another system component might be causing this problem. It might be necessary to collect and submit CDF traces to determine the nature of the failure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SessionManager.Launch.ConnectionFailed

- Description: This error is a generic failure indicating that a launch attempt has failed. Other errors sent out might indicate a cause.
- Recommended action: Look for other errors associated with the launch attempt.

SessionManager.Launch.LogonFailed

- Description: This error indicates that a connection to a remote desktop or application was established. However, the session disconnected without completing Windows (or other operating system) login.
- Recommended action: This error indicates some login failure, possibly including a failure of the user to manually enter credentials. Investigate how the user attempted to sign into the remote VDA.

SessionManager.Launch.Cancelled

- Description: The Citrix engine's connect attempt was canceled, most likely by user action.
- Recommended action: This error indicates why a connection wasn't successfully established, but likely indicates correct behavior.

SessionManager.LeaseResolution.Failed

- Description: Indicates that an offline (also called "lease-based") launch failed. This failure is because a valid and required lease for the resource wasn't found on the client machine. Also, the Gateway or Cloud Connector rejected the launch request, or the launch request was somehow invalid.
- Recommended action: Verify that the leases have been synced to the client machine, and are still valid. User can sign into their store in online mode to trigger the (re-) sync of leases. Look for the errors that the Gateway or Cloud Connector components sent. These errors might indicate reasons for the failure.

SessionManager.clxmtp.SoftDeny

- Description: A lease launch was attempted, and a Connector or Gateway informed the client that it can't complete the requested launch. However, the other Connectors or Gateways might be able to help the launch.
- Recommended action: This error doesn't indicate that the launch must fail. It indicates that the engine can't succeed through a specific network path. Look for errors that the Gateway or Cloud Connector components sent. These errors might indicate reasons for the failure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SessionManager.clxmtp.SoftDeny_Implicit

- Description: A lease launch was attempted, and a Connector or Gateway was unreachable. However, other Connectors or Gateways might be able to help the launch.
- Recommended action: This error doesn't indicate that the launch must fail. It indicates that the engine can't succeed through a specific network path. Investigate why the client can't contact a Connector or Gateway. It might be expected for that host to be inaccessible because of network topology or firewall restrictions.

Transport.Connect.NoCGP_Fail

- Description: The Citrix Workspace app core (engine) components failed to connect to a VDA host through the ICA protocol (port 1494). Attempts to connect to a gateway or VDA via the CGP protocol were not attempted if this event was sent.
- Recommended action: Investigate why the client isn't able to contact a VDA through TCP or EDT.

Transport.Connect.FallbackFail

- Description: The Citrix Workspace app core (engine) components failed to connect to a VDA host through the ICA protocol (port 1494). After this failure, the Citrix Workspace app fails to connect to a Gateway or VDA through the CGP protocol (port 2598).
- Recommended action: Investigate why the client isn't able to contact a Gateway, Connector, or VDA through either TCP or EDT.

Transport.Connect.Fail

- Description: The Citrix Workspace app core (engine) components failed to connect to a Gateway or VDA through the CGP protocol (port 2598). Attempts to connect to a VDA through the ICA protocol were not attempted if this event was emitted.
- Recommended action: Investigate why the client isn't able to contact a Gateway, Connector, or VDA through either TCP or EDT.

Windows Prelaunch

CWA-ICADOWNLOAD_ERR_00001

- Description: Unable to connect to store because of no response from the Citrix Workspace app.
- Recommended action: Verify whether Citrix® StoreFront Cloud or Citrix StoreFront is down. Also, verify the internet connectivity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CWA-ICADOWNLOAD_ERR_00002

- Description: User has canceled the session launch.
- Recommended action: Relaunch the session after sometime.

CWA-ICADOWNLOAD_ERR_00003

- Description: Unable to connect to store. Verify that the server certificates are valid.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00004

- Description: The resource to launch does not exist, not enabled, or not visible to a user.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00005

- Description: Workstations aren't available for this request.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00006

- Description: Server does not have the required license to do the requested activity.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00007

- Description: Server has refused connection to workstation.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00008

- Description: The requested workstation is under maintenance and is unavailable for use.
- Recommended action: Contact your IT admin with the error details.

CWA-ICADOWNLOAD_ERR_00009

- Description: Maximum session limit is reached.
- Recommended action: Reached the maximum session limit that was configured by an admin. Restart the session.

CWA-ICADOWNLOAD_ERR_000010

- Description: General error that cannot be further specified.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended action: Contact your IT admin with the error details.

Workspace

StoreLaunchIcaEndpoint.LaunchFailed

- Description: An error occurred while launching.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

StoreLaunchSessionEndpoint.BadRequest

- Description: The parameters of the launch request were invalid or empty.
- Recommended action: Contact Citrix support.

StoreLaunchSessionEndpoint.FarmUnavailable

- Description: There were no farms available for the launch.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs.

StoreLaunchSessionEndpoint.Error

- Description: There was an internal error while launching.
- Recommended action: Contact Citrix support.

StoreGetIcaFileEndpoint.BadRequest

- Description: There was no launch ticket provided in the request.
- Recommended action: Contact Citrix support.

StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed

- Description: Workspace was unable to retrieve the ICA file.
- Recommended action: Contact Citrix support.

StoreGetIcaFileEndpoint.Error

- Description: Workspace was unable to retrieve the ICA file.
- Recommended action: Contact Citrix support.

WebProxyGetLaunchStatusEndPoint.DSAuthFailure

- Description: There was an authentication problem.
- Recommended action: Try reauthenticating. Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WebProxyGetLaunchStatusEndPoint.LaunchFailed

- Description: There was an internal error while launching the application.
- Recommended action: Contact Citrix support.

WebProxyGetLaunchStatusEndPoint.ResourceNotFound

- Description: The launch failed because the application can't be found.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs and application configuration.

WebProxyLaunchIcaEndpoint.DSAuthFailure

- Description: There was an authentication problem.
- Recommended action: Try reauthenticating. Contact Citrix support.

WebProxyLaunchIcaEndpoint.LaunchFailed

- Description: There was an internal error while launching the application.
- Recommended action: Contact Citrix support.

WebProxyLaunchIcaEndpoint.ResourceNotFound

- Description: The launch failed because the application can't be found.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs and application configuration.

WebProxySessionsLaunchIcaEndpoint.SessionNotFound

- Description: Workspace was unable to reconnect to the existing HDX session. Your session might be terminated.
- Recommended action: Relaunch the application.

WebProxySessionsLaunchIcaEndpoint.DSAuthFailure

- Description: There was an authentication problem.
- Recommended action: Try reauthenticating. Contact Citrix support.

WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed

- Description: Workspace was unable to reconnect to the existing HDX session. Your session might be terminated.
- Recommended action: Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WebProxySessionsLaunchIcaEndpoint.Error

- Description: There was an internal error while reconnecting to the session.
- Recommended action: Contact Citrix support.

WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure

- Description: There was an authentication problem.
- Recommended action: Try reauthenticating. Contact Citrix support.

WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed

- Description: Workspace was unable to reconnect to the HDX session.
- Recommended action: Contact Citrix support.

WebProxySessionsGetLaunchStatusEndpoint.Error

- Description: There was an internal error while reconnecting to the session.
- Recommended action: Contact Citrix support.

DetermineGateway.Error

- Description: Workspace was unable to determine which Gateway to connect to.
- Recommended action: Verify your Gateway configuration. Contact Citrix support.

ConnectionRoutingProviderLaunch.Error

- Description: Workspace was unable to determine which Gateway to connect to.
- Recommended action: Verify your Gateway configuration. Contact Citrix support.

BrokerGetAddressCall.AnonymousPrelaunchNotSupported

- Description: Workspace can't launch the application because the farm doesn't support anonymous launches.
- Recommended action: Contact Citrix support.

BrokerGetAddressCall.LeasingError

- Description: Workspace received an error from the Citrix Virtual Apps and Desktops broker.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BrokerGetAddressCall.ServiceConnectionError

- Description: Workspace was unable to contact any Citrix Virtual Apps and Desktops broker in the farm.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

BrokerGetAddressCall.BrokerError

- Description: Workspace received an error from a Citrix Virtual Apps and Desktops broker.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

BrokerGetAddressCall.LicensingError

- Description: Workspace was unable to launch the application because of a licensing error.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

BrokerGetAddressCall.Error

- Description: Workspace can't retrieve the VDA details from the Citrix Virtual Apps and Desktops broker.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GetLaunchReference.NoAccessToken

- Description: Workspace can't successfully connect to the VDA.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GetLaunchReference.BrokerError

- Description: Workspace can't successfully connect to the VDA.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GetLaunchReference.Error

- Description: Workspace can't successfully connect to the VDA.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GenerateIcaFile.InvalidIcaSetting

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

StoreIcaFileAndGetTicket.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetFasVdaLogonTicket.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GenerateSTATicket.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetVdaAddress.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetTicket.NoAccessToken

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetTicket.BrokerError

- Description: The Citrix Virtual Apps and Desktops broker was unable to launch the HDX session.
- Recommended action: Verify the ID in the error message and Verify your Citrix Virtual Apps and Desktops logs.

GetTicket.ServiceConnectionError

- Description: Workspace can't contact a Citrix Virtual Apps and Desktops broker.
- Recommended action: Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GetTicket.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetNetscalerConfigurationByCustomer.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

DiscoverMPSServerCapabilities.Error

- Description: There was a problem making a request to the Citrix Virtual Apps and Desktops broker.
- Recommended action: Verify your Citrix Virtual Apps and Desktops logs. Contact Citrix support.

GetResourceLocationNetScalerConfig.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetCustomerResourceLocations.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetResourceLocationFromResourceProvider.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetNetScalerGatewayInfo.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetCustomerEntitlements.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

GetResourceLocationForServerFeed.Error

- Description: There was an internal error while establishing an HDX connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended action: Contact Citrix support.

GetResourceInformation.Error

- Description: There was an internal error while establishing an HDX connection.
- Recommended action: Contact Citrix support.

Citrix Gateway as a service

CGS-ICASN_ERR_00001

- Description: Application launch failed because of request parsing error.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00002

- Description: Failed to validate authentication ticket.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00003

- Description: The ICA file downloaded from browser is used for the session launch after 90 seconds, by then STA ticket expires.
- Recommended action: Retry session launch.

CGS-ICASN_ERR_00004

- Description: Failed to validate authentication ticket.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00005

- Description: Failed to establish connection to the Connector.
- Recommended action: Verify connector health. If the issue persists, contact Citrix support.

CGS-ICASN_ERR_00006

- Description: Connection request to the Connector timed out.
- Recommended action: Verify connector health. Verify if any proxy settings blocks traffic between connector/VDA and NGS. Verify connectivity between VDA and Connector. If the issue persists, Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CGS-ICASN_ERR_00007

- Description: The connection is closed by Citrix Workspace app on the Client Machine before session was established.
- Recommended action: Retry session launch.

CGS-ICASN_ERR_00008

- Description: Back-end closed the connection.
- Recommended action: Verify connector health. Verify network stability from Connector/VDA to public network(NGS). If the issue persists, contact Citrix support.

CGS-ICASN_ERR_00009

- Description: Failure in VDA to NGS connection establishment (Rendezvous).
- Recommended action: Verify the connector health. VDA must be able to reach NGS Service. Verify connectivity between VDA and Connector. If the issue persists, contact Citrix support.

CGS-ICASN_ERR_00010

- Description: EDT to TCP fallback. Verify prerequisite for EDT.
- Recommended action: Rendezvous must be enabled and VDA must be able to reach NGS service over UDP. If the issue persists, contact Citrix support.

CGS-ICASN_ERR_00011

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00012

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00013

- Description: Failure in GCT validation.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00014

- Description: Failure in GCT validation.
- Recommended action: Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CGS-ICASN_ERR_00015

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00016

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00017

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00018

- Description: Failed to validate authentication ticket.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00019

- Description: Failed to validate authentication ticket.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00020

- Description: Error in CGS internal licensing.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00021

- Description: Rendezvous v2 fall back because of disabled feature flag.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00022

- Description: Failure in NGS internal service.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00023

- Description: Timeout in CLXMTP exchange.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended action: Verify that the connectors are healthy and reachable to NGS service. If the issue persists, contact Citrix support.

CGS-ICASN_ERR_00024

- Description: Failure in CLXMTP VSR validation.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00025

- Description: Failure in CLXMTP VSR validation.
- Recommended action: Contact Citrix support.

CGS-ICASN_ERR_00026

- Description: Connector isn't available in CLXMTP.
- Recommended action: Verify whether the connector is in the healthy state for the resource location. If the issue persists, contact Citrix support.

CGS-ICASN_ERR_00027

- Description: CLXMTP redirect to Connector failed after maximum trials.
- Recommended action: Verify whether the connector is in the healthy state for the resource location. Verify that the `Citrix ClxMtp Service` service is running in all connectors. Contact Citrix support.

CGS-ICASN_ERR_00028

- Description: Failed to communicate with the Controller.
- Recommended action: Contact Citrix support.

Success: CGS_ICASN_SUCCESS_00001

- Description: Session launch request received.
- Recommended action: Not applicable

Success: CGS_ICASN_SUCCESS_00002

- Description: Session launch request completed.
- Recommended action: Not applicable

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XAXD proxy

XDPXY_INF_00001

- Description: Broker sends a request to the VDA to prepare for incoming connections.
- Recommended Action: Not applicable

XDPXY_INF_00002

- Description: VDA confirms request for connection by Broker.
- Recommended Action: Not applicable

XDPXY_ERR_00001

- Description: Failed to communicate with the VDA.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00002

- Description: XaxdProxy timed out waiting for a response from VDA.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00003

- Description: Encountered a WCF fault or exception while trying to make the request.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you have a web proxy between the Connector and Broker, make sure it is properly configured.
- If the issue persists, contact Citrix support.

XDPXY_INF_00003

- Description: Request for validation for an incoming ICA or RDP connection is called by the stack.
- Recommended Action: Not applicable

XDPXY_INF_00004

- Description: Validation of the incoming ICA or RDP connection is established.
- Recommended Action: Not applicable

XDPXY_ERR_00001

- Description: Failed to communicate with the VDA Proxy.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00002

- Description: XaxdProxy timed out waiting for a response from VDA Proxy.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00003

- Description: Encountered an exception while trying to make the request.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Restart Citrix Delivery Agent service on VDA or restart VDA.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_INF_00005

- Description: Request for HDX session traffic direct to VDA is made.
- Recommended Action: Not applicable

XDPXY_INF_00006

- Description: VDA establishes direct connection with Citrix Cloud™ control plane for HDX session traffic.
- Recommended Action: Not applicable

XDPXY_INF_00007

- Description: Client sends connection request to on-premises StoreFront for a resource.
- Recommended Action: Not applicable

XDPXY_INF_00008

- Description: On-premises StoreFront accepts connection request from client for resource.
- Recommended Action: Not applicable

XDPXY_ERR_00004

- Description: XaxdProxy got an HTTP error response while trying to connect.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - Verify network stability from Connector to public network.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XDPXY_ERR_00006

- Description: The XML request has an invalid format.
- Recommended Action: Contact Citrix support

XDPXY_ERR_00007

- Description: XML request has invalid credential headers and/or format.
- Recommended Action: Logout, login again, and retry action. if the issue persists, contact Citrix support

XDPXY_INF_00011

- Description: Service continuity launch is requested by the user via WSA.
- Recommended Action: Not applicable

XDPXY_INF_00012

- Description: Service continuity launch is requested by the user via WSA.
- Recommended Action: Not applicable

XDPXY_ERR_00004

- Description: XaxdProxy encountered an HTTP error while trying to connect.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

XDPXY_ERR_00008

- Description: Service continuity launch failed as XaxdProxy timed out waiting for a response.
- Recommended Action: Check the health of the Connector. For more information, see Citrix Cloud Connector and CTX224133.
  - If you have a web proxy between the Connector and Broker, make sure it is properly configured.
  - If the issue persists, contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XDPXY_ERR_00009

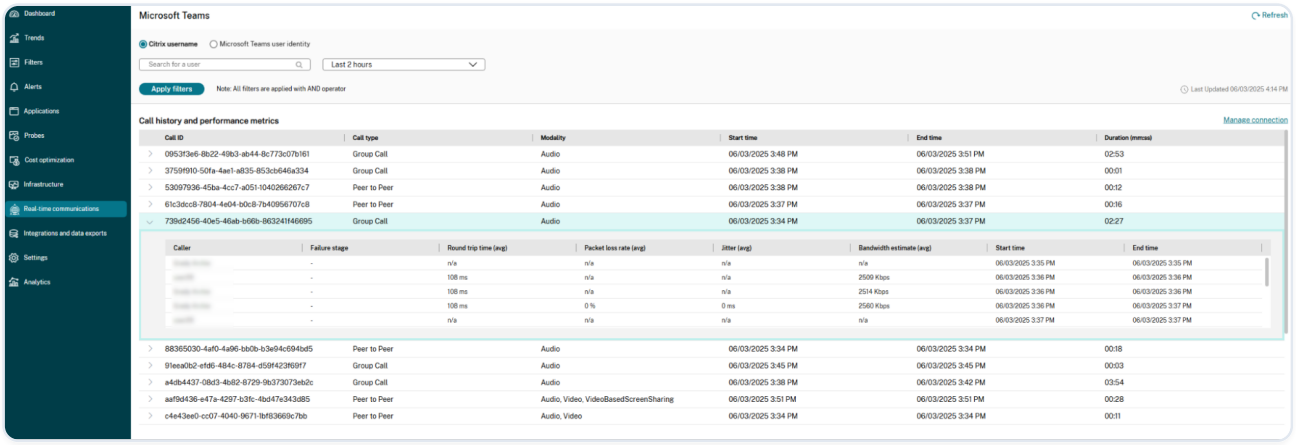
- Description: Service continuity launch failed due to the lease being blocked and/or revoked.
- Recommended Action: Contact your Citrix Cloud Administrator with the error details. For more information, see Service continuity documentation.
    - If the issue persists, contact Citrix support.

Real time communications dashboard

Microsoft Teams

Microsoft Teams dashboard in Citrix Director provides visibility into Microsoft Teams calls across users along with details on the participants and metrics that indicate call performance. The dashboard provides the ability to:

- Assess Microsoft Teams usage summary
- Filter and see details of Microsoft Teams calls for the selected duration
- Assess individual calls using performance metrics



Prerequisites

Add Microsoft Graph Application Programming Interface (API) to the allow list in Citrix Director:

- For Director to access call records, ensure outbound internet access is available on all the machines where Director is installed. Specifically, ensure the `https://graph.microsoft.com` URL is accessible
- If you use a proxy server, ensure that the Microsoft Graph API : `https://graph.microsoft.com` URL is accessible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Getting started

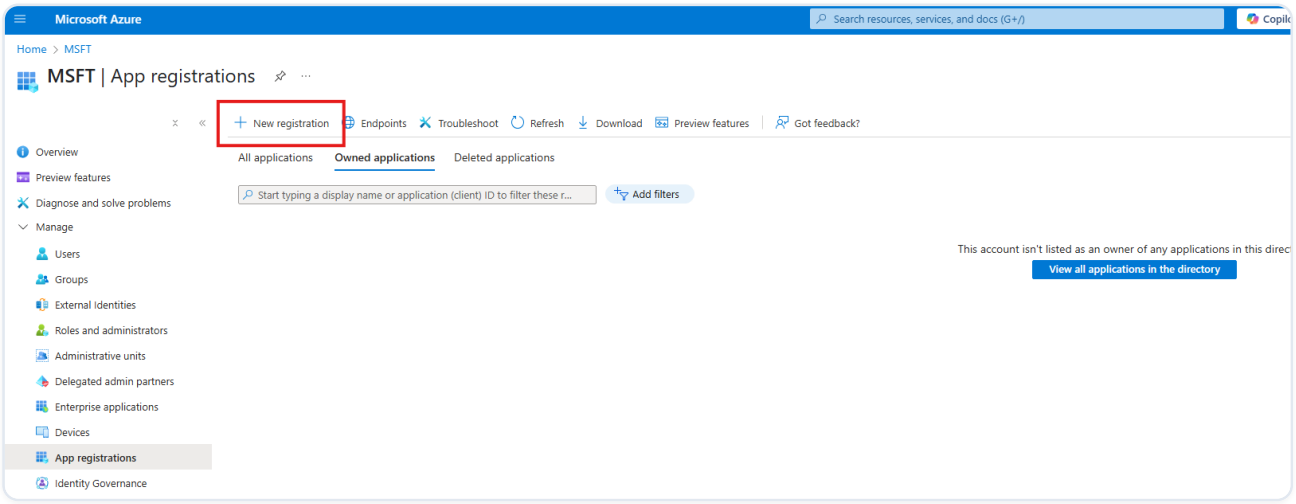
Connection to Microsoft Graph API

The Microsoft call details are fetched from the Microsoft Graph API. For Citrix Director to access the API, an app needs to be created in the Microsoft Entra ID with the required permissions. The Graph API URL needs to be added to the allow list in Director as well.

Perform the following steps to complete the connection:

Step 1: Application registration in Microsoft Entra ID

1. Navigate to **App registrations -> New registration** in Microsoft Entra ID.

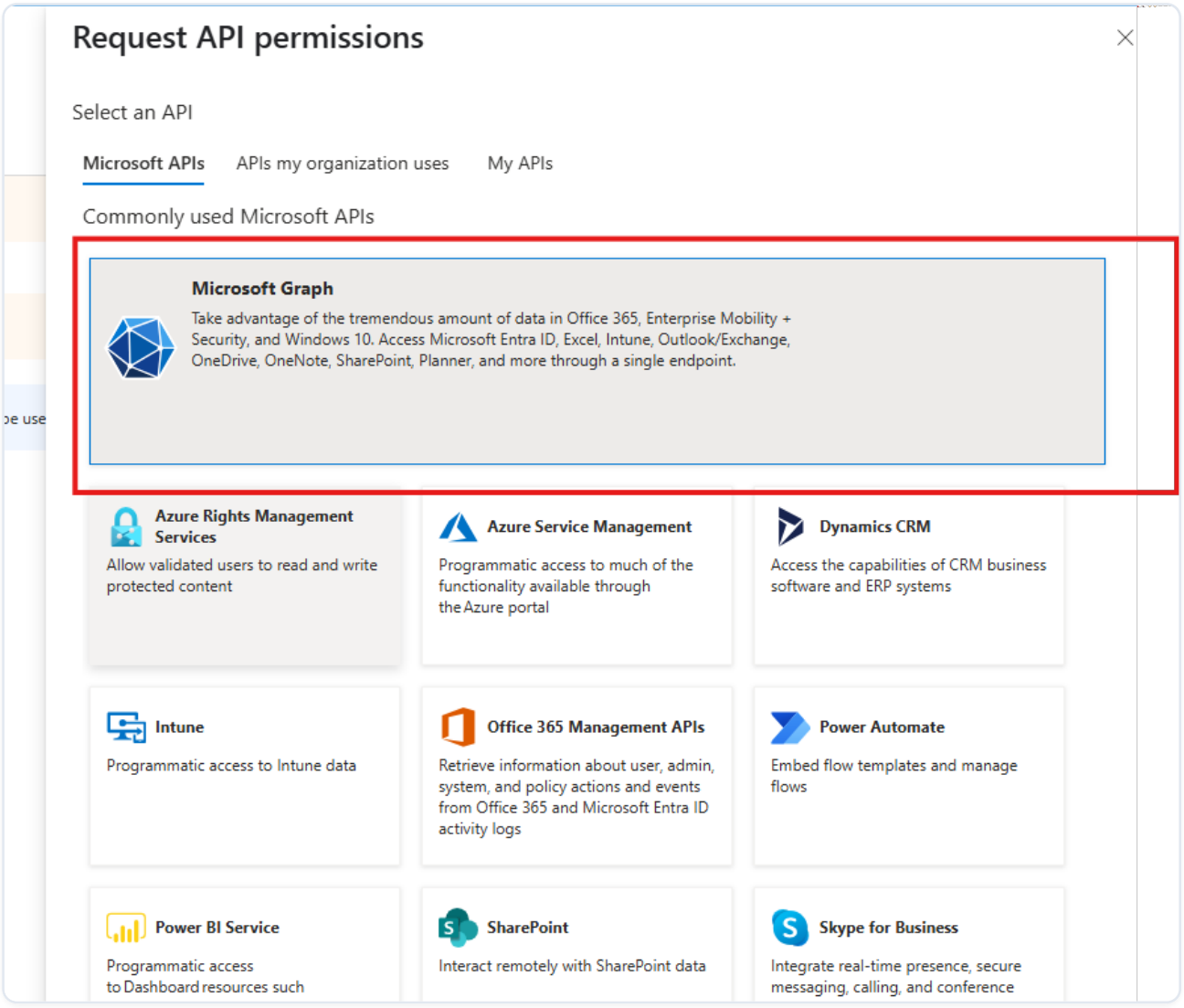


1. Perform the required steps for app registration.
2. After registration, copy the Client ID and Tenant ID of the application.

STEP 2: ADDING MICROSOFT GRAPH PERMISSIONS IN MICROSOFT ENTRA ID

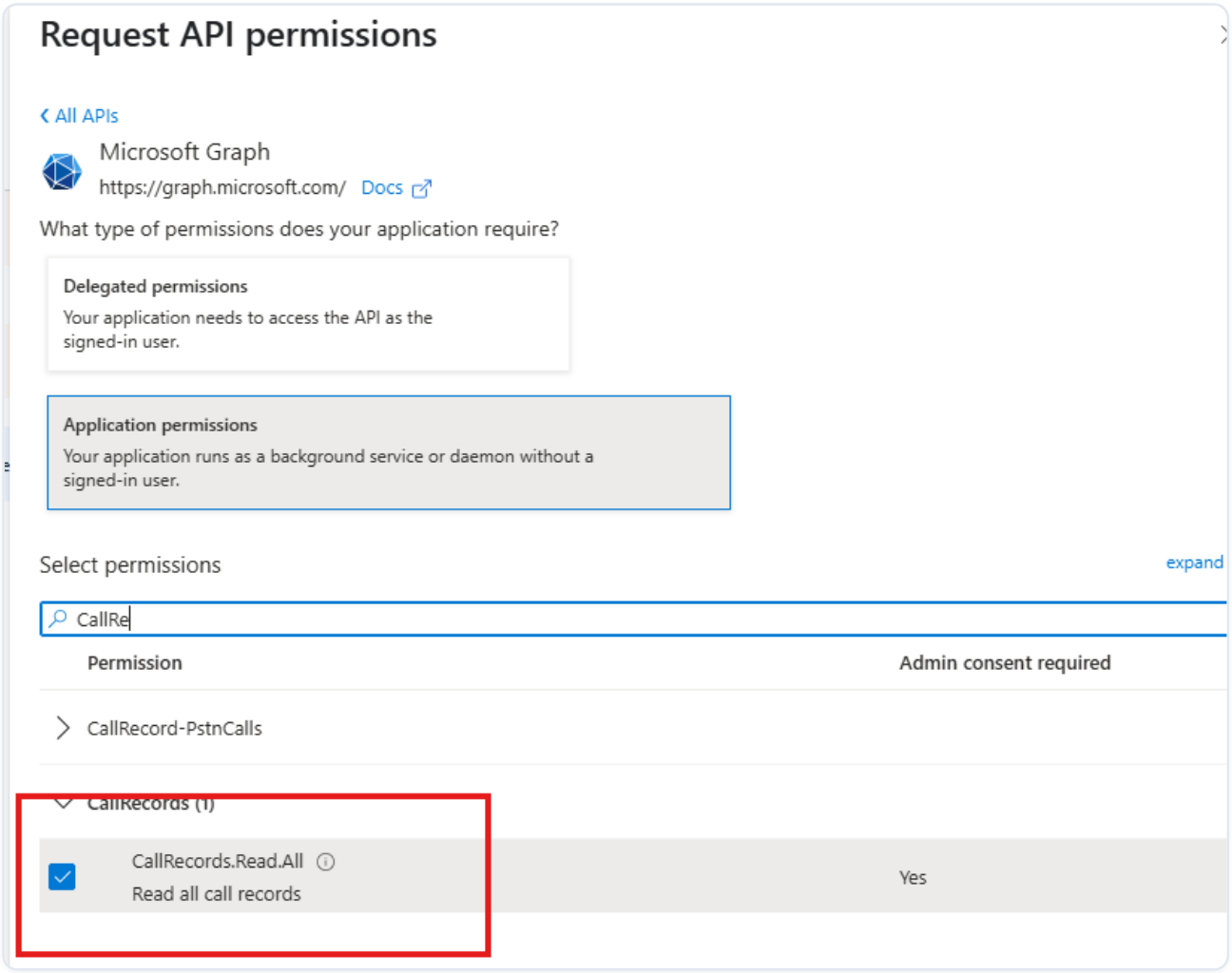
1. Navigate to **API permissions -> Add a permission.**
2. Select **Microsoft Graph** and then **Application permissions.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

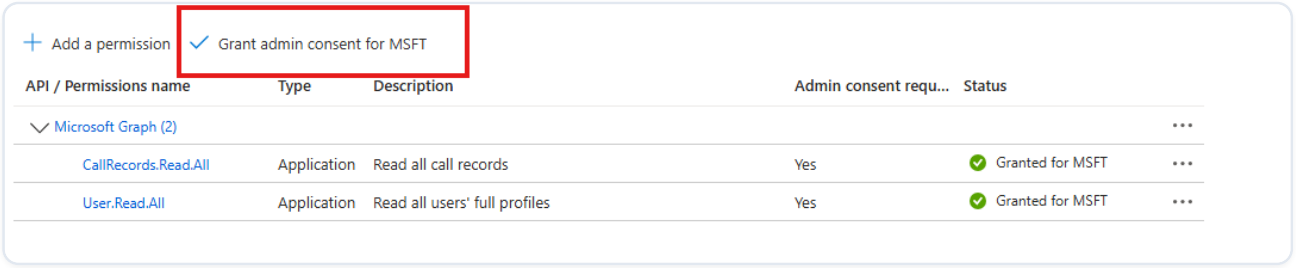


1. Add permissions to **CallRecords.Read.All** and **User.Read.All**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



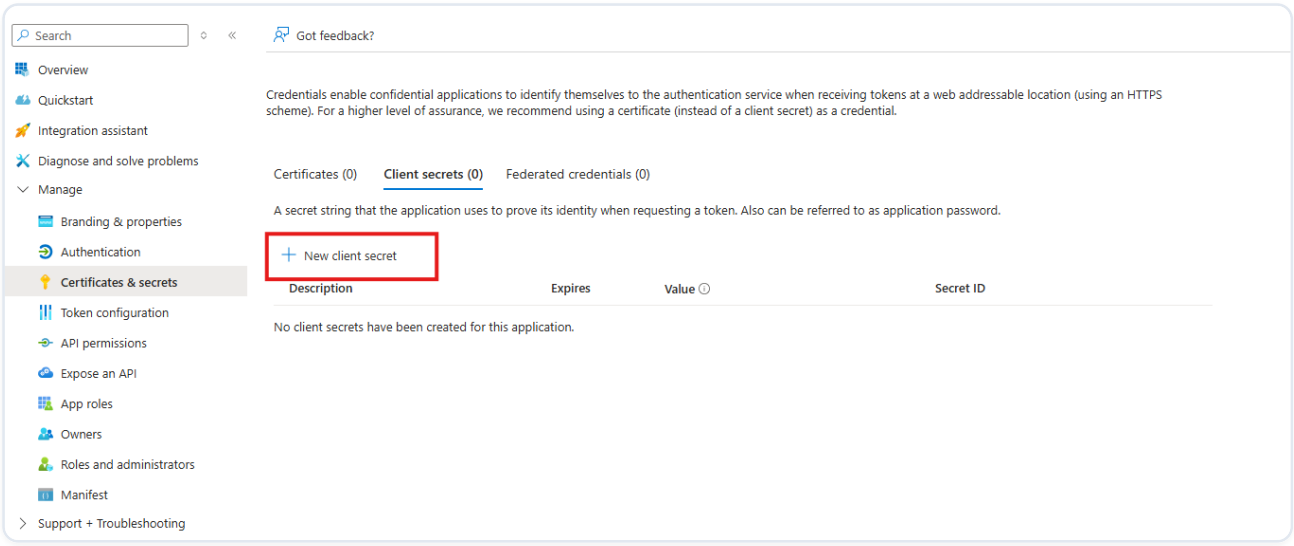
1. Click Grant admin consent for MSFT. This action requires an Entra ID global administrator.



Step 3: Creating a Client Secret

1. In Microsoft Entra ID, navigate to **Certificates & secrets > New client secret**. You can also re-use an existing secret.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

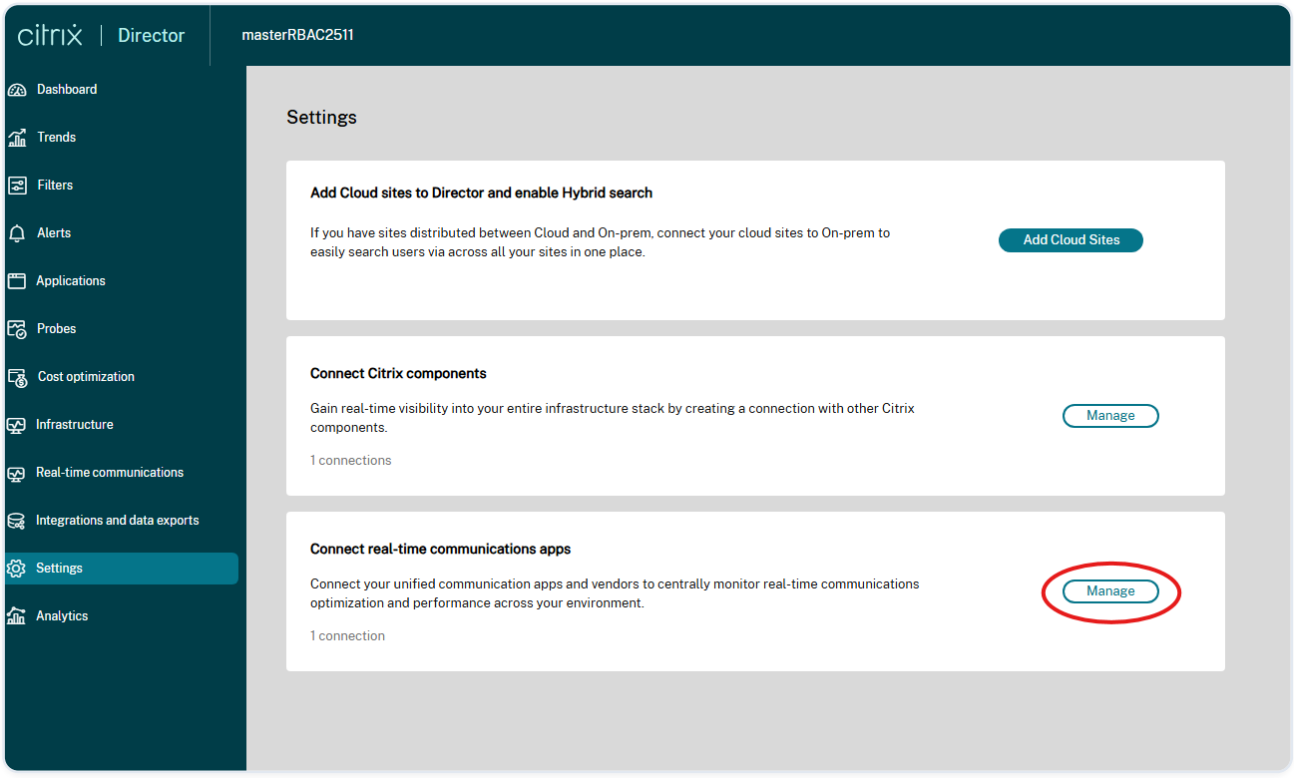


1. Provide a name and expiration date for the secret. Ensure that the secret is renewed before expiration to maintain the connection.
2. Copy the client secret for use in the Director UI.

For more information, see the official Azure documentation if you face any issues.

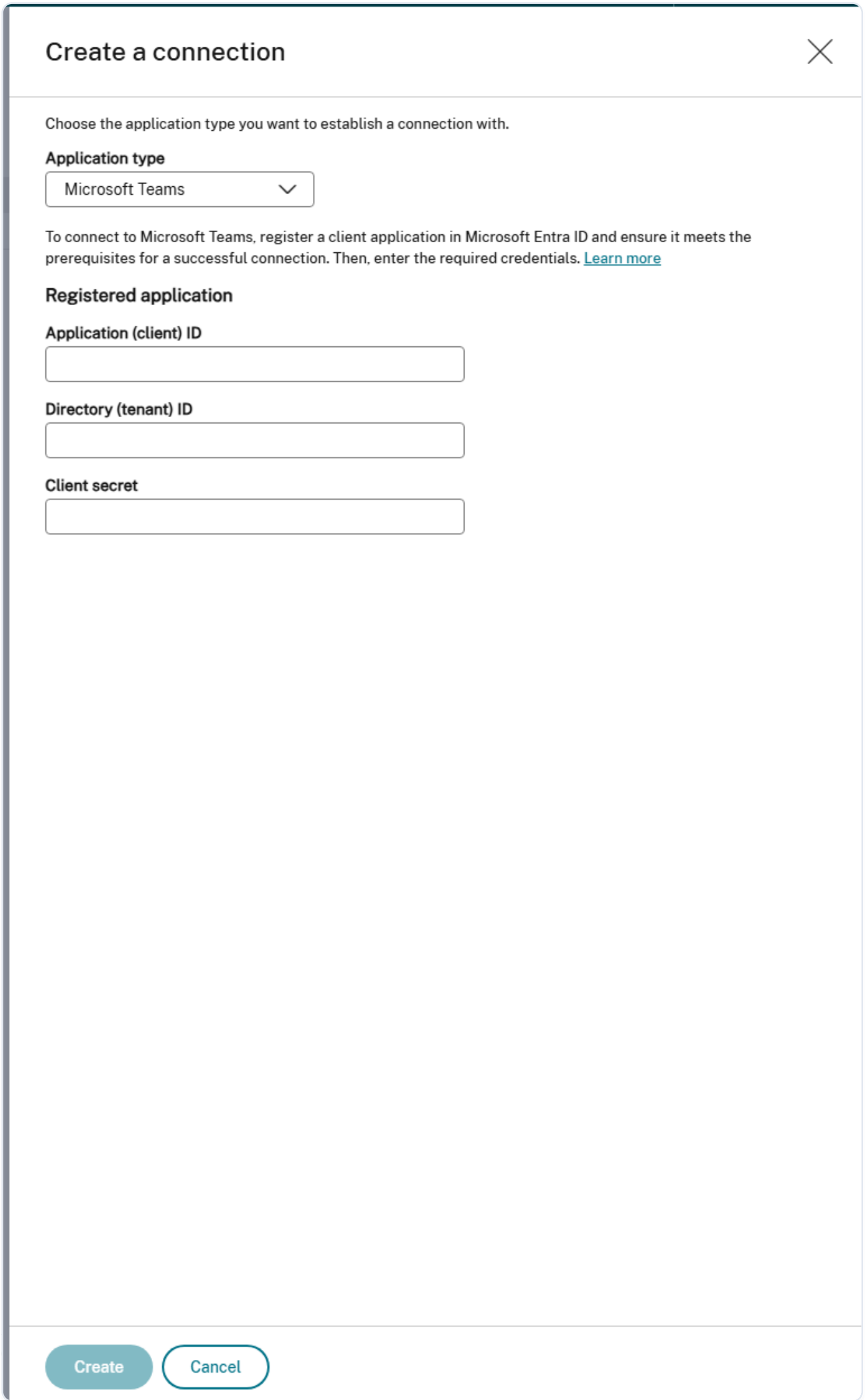
Step 4: Complete Connection on Director

1. In Director, navigate to **Settings -> Connect real-time communications apps**.

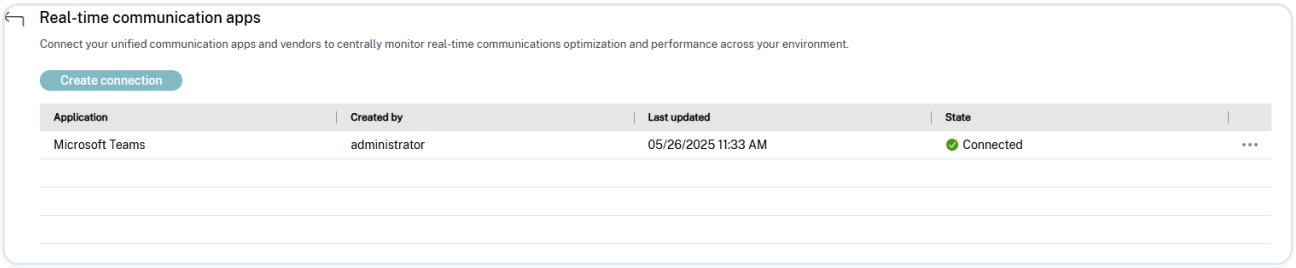


1. Click **Create connection** and enter the copied Application ID, Directory ID, and Client Secret from the app registration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Create a connection
Choose the application type you want to establish a connection with.
Application type
Microsoft Teams
To connect to Microsoft Teams, register a client application in Microsoft Entra ID and ensure it meets the prerequisites for a successful connection. Then, enter the required credentials. Learn more
Registered application
Application (client) ID
Directory (tenant) ID
Client secret
Create
Cancel

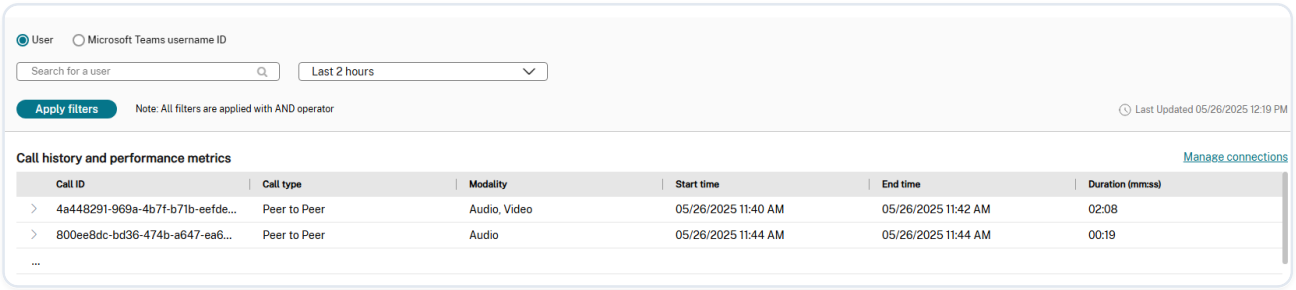
Connection is successfully established if valid credentials and permissions to fetch call details are available.



1. You can **Edit** and **Delete** the connection by clicking the ellipse at the end of the row.

Microsoft Teams dashboard

Navigate to **Real time Communications** tab in the Director UI. The Microsoft Teams dashboard is populated with the data collected from the Microsoft Graph connection established. Call details are available approximately 15 minutes after the call ends.

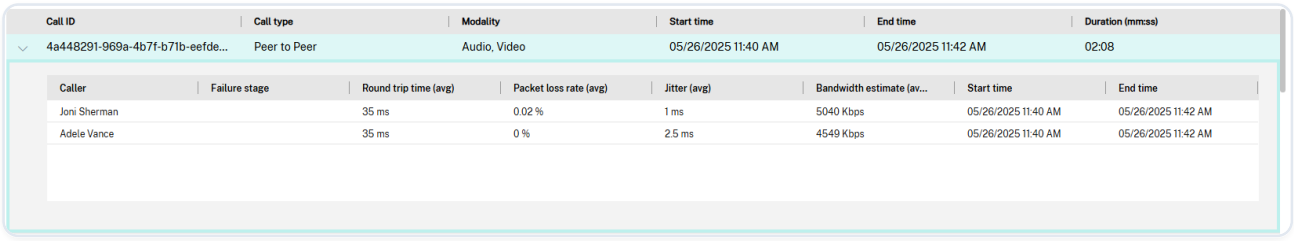


The table view provides the following details across all calls.

COLUMN NAME	DESCRIPTION
Call ID	A unique identifier for each call.
Call type	Indicates whether the call is peer-to-peer or a group call.
Modality	Indicates which modes are used during the call, such as audio, video, or screen share.
Start time	The date and time the call began.
End time	The date and time the call ended.
Duration (mm: ss)	Duration of the call in minutes and seconds.

Click individual calls in the table to view the failure and performance details per user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Call ID	Call type	Modality	Start time	End time	Duration (mm:ss)
4a448291-969a-4b7f-b71b-eefde...	Peer to Peer	Audio, Video	05/26/2025 11:40 AM	05/26/2025 11:42 AM	02:08

Caller	Failure stage	Round trip time (avg)	Packet loss rate (avg)	Jitter (avg)	Bandwidth estimate (av...	Start time	End time
Joni Sherman		35 ms	0.02 %	1 ms	5040 Kbps	05/26/2025 11:40 AM	05/26/2025 11:42 AM
Adele Vance		35 ms	0 %	2.5 ms	4549 Kbps	05/26/2025 11:40 AM	05/26/2025 11:42 AM

In a group call, when a user disconnects and rejoins, it is considered as a separate session. This consideration helps to identify specific issues, such as higher latency when connected to a particular network.

Each row in the call details table contains the following information:

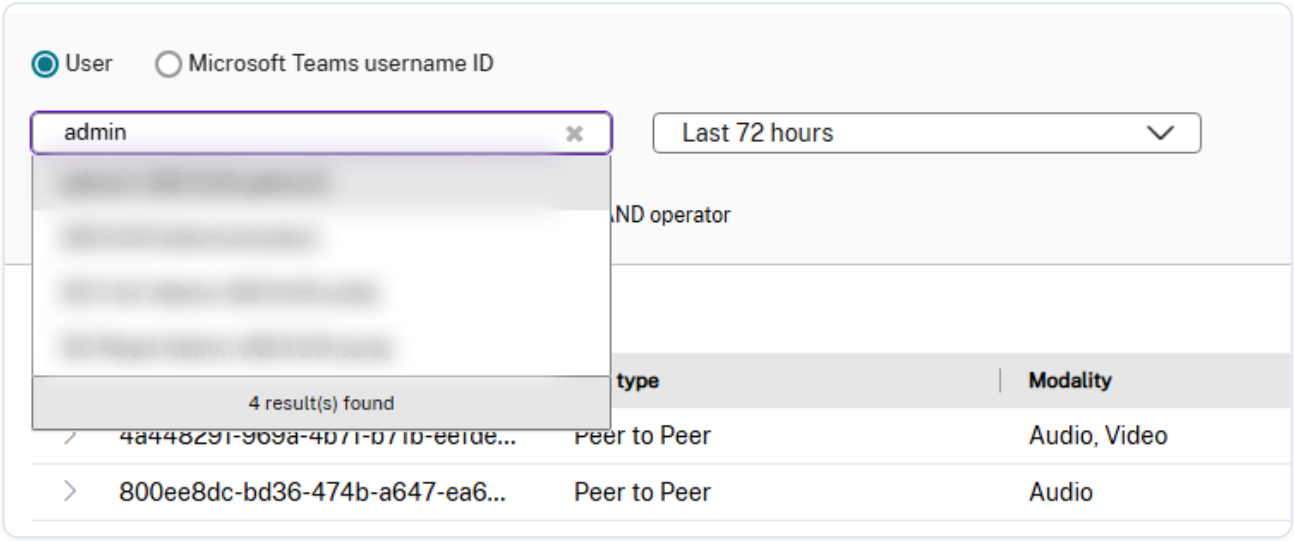
COLUMN NAME	DESCRIPTION
Start time	The date and time the call or participant's segment began.
Round trip time (avg)	Average round-trip time for data packets.
Packet loss rate (avg)	Average percentage of packets lost during the call.
Jitter (avg)	Average variation in the delay of received packets.
Failure stage	Indicates the stage at which a call failure occurred, such as during setup or in the middle of the call.
End time	Date and time the call or participant's segment ended.
Caller	Name of the participant in the call.
Bandwidth estimate (avg)	Estimated average bandwidth used during the call.

You can filter users in two ways: by Citrix user name or by Microsoft Teams user name. You can switch between these options using the radio buttons at the top of the page.

- **Citrix user name:** As you begin typing a user name, the system suggests matching users. You can then select the specific account to view details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Microsoft Teams User name:** Use this option if the email or User Principal Name (UPN) associated with the Microsoft Teams account differs from the Citrix account ID. When using this method, you must enter the complete and valid email address.



Service continuity monitoring dashboard

Overview

The Service Continuity Monitoring Dashboard provides administrators with centralized, immediate visibility into configuration gaps and end-user vulnerabilities that could prevent Service Continuity from functioning during a cloud outage. By monitoring readiness, administrators can use the readiness data for early detection, take corrective actions to ensure users maintain access to their applications and desktops, ultimately reducing the business impact of outages.

What is an instance, and how is data collected from it?

An instance represents a unique way a user accesses Citrix Workspace™, based on the user, the device, and how they sign in. For example, if a user signs in on one device using Chrome, Edge, and the Citrix Workspace app, each access method is tracked as a separate instance. Each instance sends an event approximately once every 24 hours.

How readiness is calculated

For an instance to be considered ready, it must satisfy the following conditions. If any of them is not met, the instance is considered "Not ready".

For native app launch

- Service continuity is enabled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- At least one leasable resource (app or desktop) is available
- At least one valid connection lease exists
- No expired connection leases are present

For hybrid launch (login from web, session launch via CWA app)

- Service continuity is enabled
- Citrix web extension is installed
- At least one leasable resource (app or desktop) is available
- At least one valid connection lease exists
- No expired connection leases are present

Version requirements

Service continuity readiness data is available with certain Citrix Workspace app versions and above.

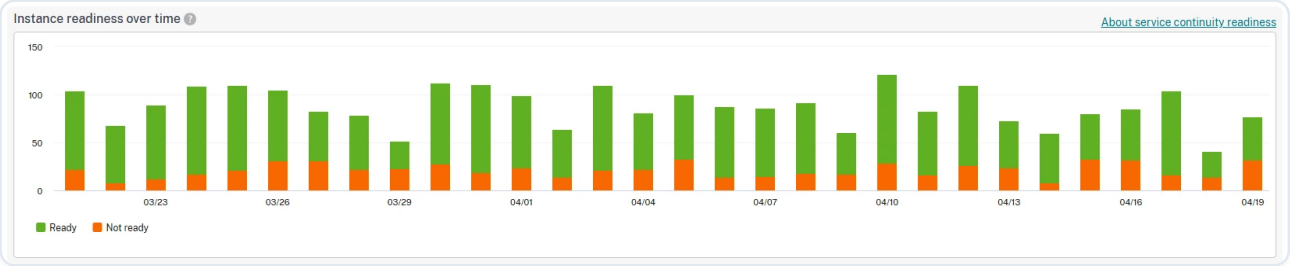
PLATFORM	MINIMUM SUPPORTED VERSION
Hybrid (login from web, session launch via CWA app)	Automatically updated
CWA Windows	2511
CWA Mac	2603
CWA Linux	2503
CWA Android	2603
CWA iOS	2603

Dashboard features

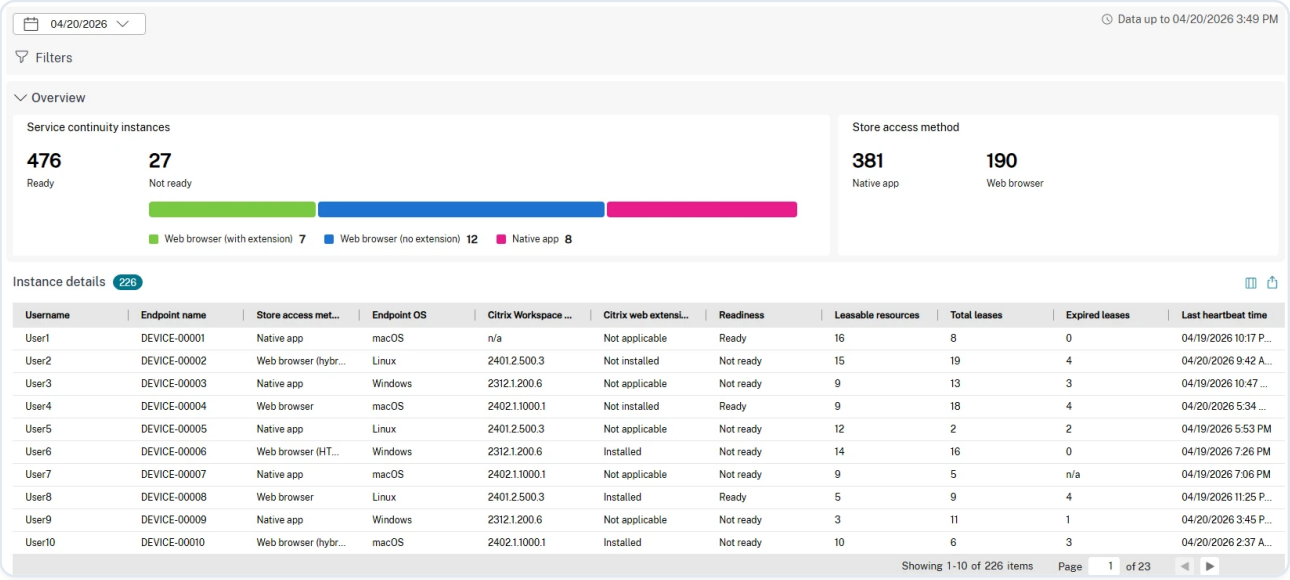
Instance readiness over time chart

A 30-day readiness bar graph that represents the readiness count on each day. The green section represents the "Ready" instances, while the orange section represents the "Not ready" instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Day-wise overview panel and instance charts



These two sections represent the data corresponding to a single day. By default, the current day is selected. Users can see the day-wise data for up to the last 7 days, and can slice and dice this data using different filters. Day-wise data is limited to 7 days because individual instance records are retained for that period, while the daily summaries behind the 30-day chart are retained for 30 days.

The current day is still in progress. Because each instance reports approximately once every 24 hours, today's counts build up over the course of the day and are lower than those of a completed day. Select a previous day for a complete view.

Overview panel

The overview panel contains the following subsections:

1. **Service continuity instances**

   It shows the count of Ready and Not ready instances. A chart is displayed below the "Not ready" section, showing a platform-wise split of the not ready instances.

2. **Store access method**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This section represents the day-wise split of the user store access method. Native app represents logins from the Citrix Workspace app on platforms such as Windows, Linux, and Android, while Web browser shows store logins through a browser or HTML5 platforms.

Instance details

Instance details consist of all the readiness events received over the course of the selected day. Each row represents a single instance. The table can also be exported as a CSV file.

Filters

The data can be filtered using the date filter and filters based on data fields. The following data fields are supported:

- Citrix Workspace app version
- Endpoint OS
- Readiness
- Store access method

Table fields

The columns are grouped into User, Endpoint, and Service continuity. Use **Manage columns** to add or remove the optional ones.

CATEGORY	FIELD	INFO	VISIBLE BY DEFAULT
User	Username	The user's username	Yes
Endpoint	Endpoint name	The hostname of the user's endpoint	Yes
Endpoint	Store access method	How the user is accessing the store - CWA app or via a browser	Yes
Endpoint	Endpoint OS	Endpoint OS platform (Windows, macOS, Android, and so on)	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

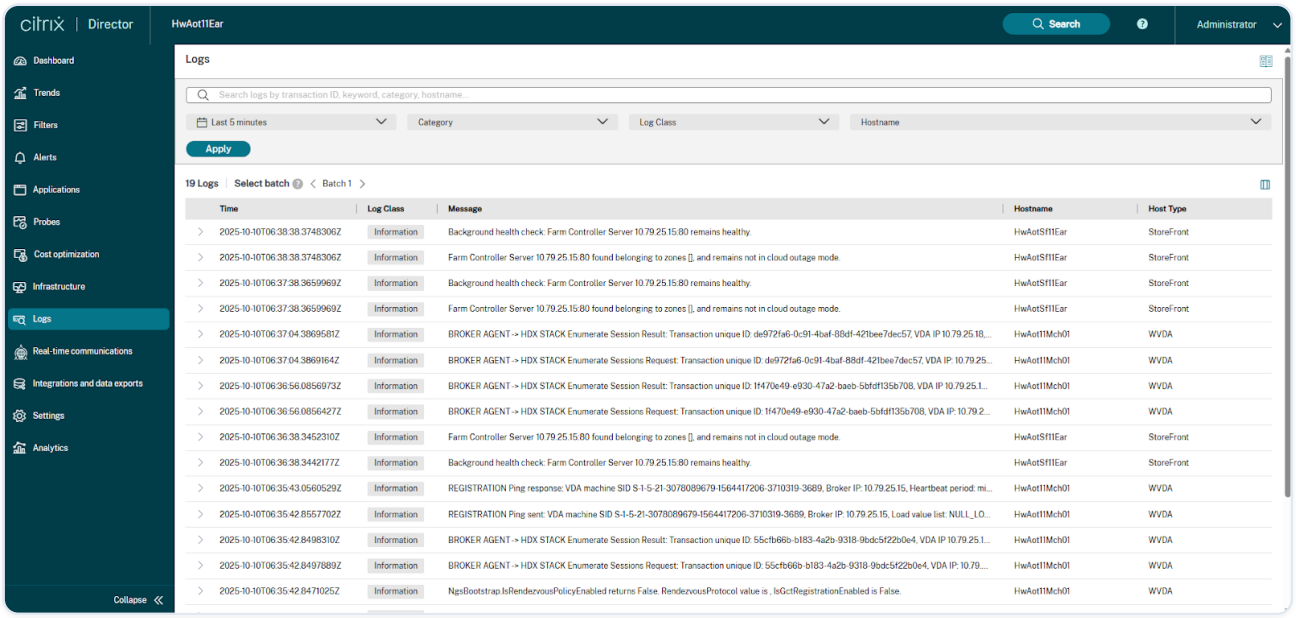
CATEGORY	FIELD	INFO	VISIBLE BY DEFAULT
Endpoint	Citrix Workspace app version	The version number of the installed native app	Yes
Endpoint	Citrix web extension	Denotes whether the user has installed the Citrix web extension. It is "not applicable" for a pure native launch	Yes
Service continuity	Readiness	Readiness based on the formula explained above (Ready/Not ready)	Yes
Service continuity	Leasable resources	The count of leasable resources (apps and desktops) the user has access to. These can be launched in a partial outage scenario	Yes
Service continuity	Total leases	Count of total leases on the user's device when the sync happened	Yes
Service continuity	Expired leases	Count of expired leases on the user's device when the sync happened	Yes
Service continuity	Last lease sync	The last time the user's device synced the lease files. By default, lease sync happens every 6 hours	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	FIELD	INFO	VISIBLE BY DEFAULT
Service continuity	Last heartbeat time	The timestamp when the user data was synced with the dashboard. Every instance sends a heartbeat with all the relevant information approximately once every 24 hours	Yes

Logs

The new Logs View in Citrix Director/Monitor is designed to surface Always On Tracing (AOT) to significantly enhance an administrator's ability to diagnose and resolve customer issues within Citrix Virtual Apps and Desktops (CVAD) environments. By integrating with your Centralized Log Server, this feature provides a unified, searchable view of AOT logs across various core components, including Virtual Delivery Agents, Delivery Controllers, StoreFront and other Citrix components. This centralized access streamlines troubleshooting by allowing for quick log retrieval and analysis from a single console.



Learn more about the architecture and benefits of Always On Tracing (AOT) in the product documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites and Configuration

To effectively use the “Logs” view in Director, your environment needs to be configured correctly and fulfill the necessary prerequisites.

- **CVAD Version Requirement**: You must be running CVAD 2507 CU1 or CVAD 2511 (or a later version).
- Centralized Log Server: Your customer-managed Resource Location must host a Centralized Log Server. Learn more about Installing and Configuring your Log Server
- When the log server is configured in HTTPS mode (e.g., `https://<LogServerFQDN>:port`), it is essential to install and trust the necessary certificate on both the Director and DDC machines. This certificate must be managed by the computer account on each machine.
- **Cloud Connector Requirement**: Cloud Monitor retrieves AOT logs through the **Monitor Connector service running on a supported Windows Cloud Connector** in the Resource Location. A supported Windows Cloud Connector must also be present in the same Resource Location. The Cloud Connector must be running version **6.141.0.13739** (or **4.420.0.13739**) or later.

Getting Started

Once the prerequisite configurations are complete, the new Logs tab in the Director UI, will provide unified visibility to your centralized AOT logs.

Accessing the Logs View

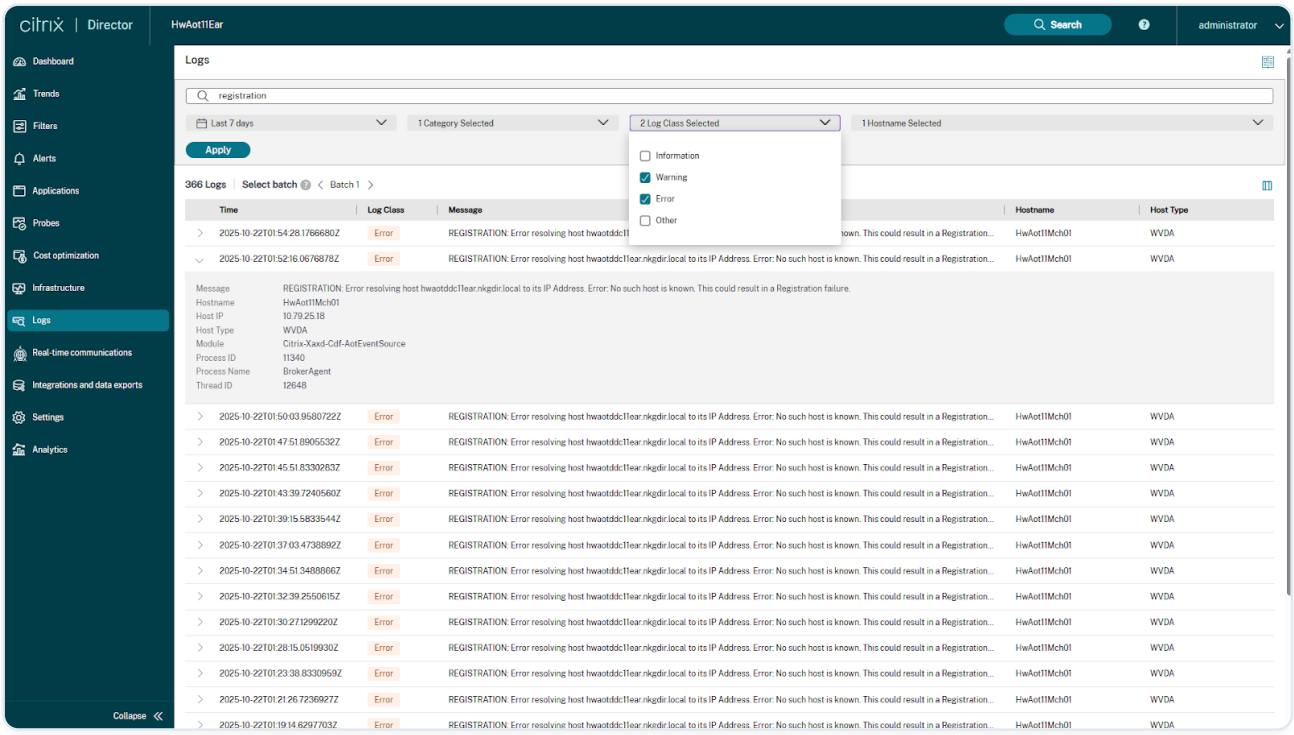
The Logs View can be accessed directly as a dedicated tab within Director, or contextually navigated to from other key troubleshooting areas:

- **Dedicated “ Logs” Tab**: Access the new "Logs" page directly in the Director/Monitor interface using the navigation panel.
- **Activity Manager**: Click an option to view related logs for the machine hosting the session.
- **Machine Filters**: Click an option to view related logs with a pre-filled Machine name.

Using the Logs View

The Logs View is designed for flexible and powerful log search, enabling administrators to quickly pinpoint relevant events.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The main search interface includes:

- **Search Bar**: A powerful text box allowing you to search by any keyword. Common search terms include Transaction ID, Session ID, User Name, or specific error messages.
- **Filter Selectors**: Use the following drop-down filters to narrow your search scope:
- **Time Interval**: Filter logs by a specific time range.
- **Category**: Filter by log category.
- **Log Class**: Filter by the class of the log message (e.g., AOT_INFO).
- **Machine name**: Filter logs originating from a specific machine name.

Search results are presented in a comprehensive table format with key attributes such as Time, Message, HostName, Level, Module, ProcessId, and more. You can expand individual log entries to view full details. Director supports configuring and viewing custom columns relevant to your log data. Additionally, results are paginated for easy viewing and navigation of large data sets.

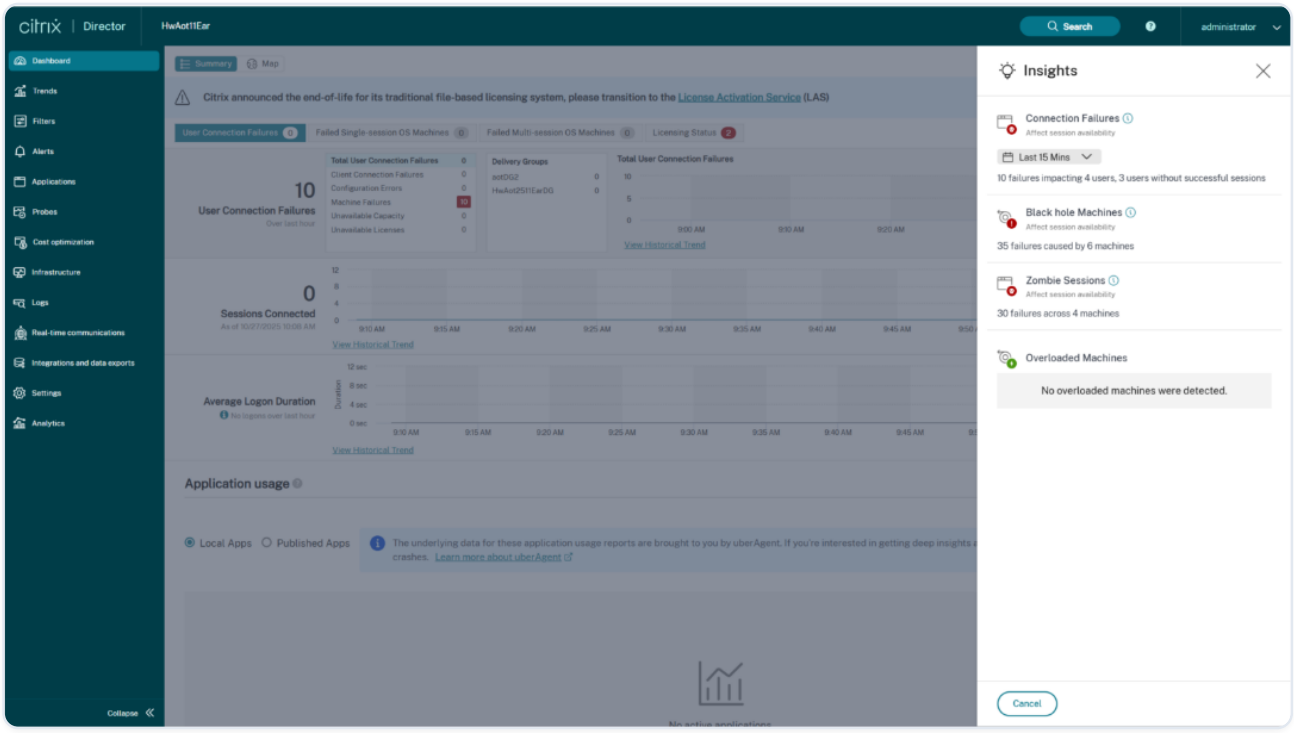
By providing immediate, context-aware access to all AOT logs, this feature aims to reduce the time spent switching between tools and manually correlating logs, leading to faster issue resolution.

Insights

The Insights panel provides information regarding session failures or slowness in your environment. Drilling deeper into specific metrics with these insights helps troubleshoot and resolve session failures or slowness faster. Failure Insights specifically help administrators to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

improve the session availability, which is an important factor that determines user experience. These insights are designed to aid in proactive monitoring of the user experience. Hence, Insights are displayed for the current failures in the system (refreshed every 15 minutes).



Clicking the insights icon from the Dashboard displays the insights pane with details about the insights and options to drill down to the Machines or Connections view. Admin can also navigate to alert configuration from the panel.

Blackhole Machines, Zombie Sessions, Overloaded Machines, and Session failure Insights are available on this panel. Each insight upon expansion displays a link to the failed sessions or the machines hosting them. This leads to the Filters view containing the failed machines or sessions. Further drill-down is possible from here when you click on a specific machine or session to see the detailed metrics.

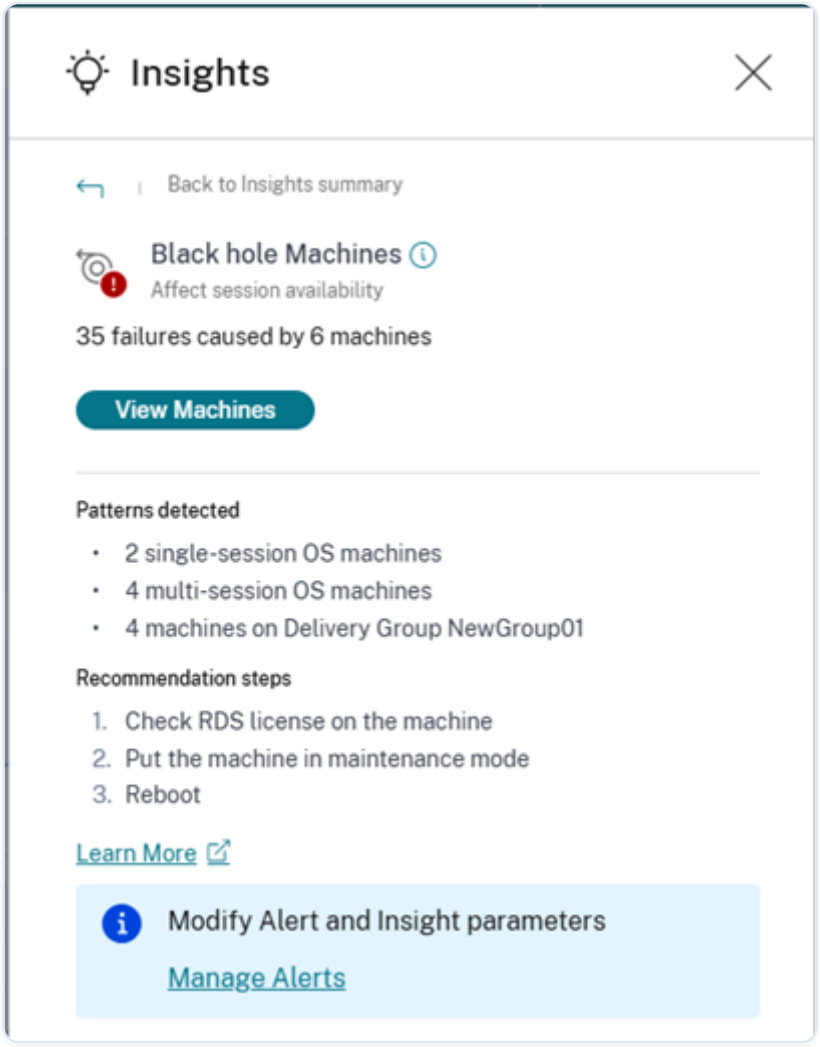
The expanded view for each insight shows top failure patterns detected with respect to the site, Delivery Group, single or multi-OS session machines. These patterns are aimed at helping administrators spot if there is a specific cohort of users experiencing the issue. In cases where the system is unable to highlight any patterns due to a distributed cohort, it is recommended to drill down to self-analyze. Also, actions that are recommended to be taken to troubleshoot and resolve the issues are shown.

Black hole machines

Some machines in your environment though registered and appearing healthy might not service sessions brokered to them, resulting in failures. Machines that have failed to service four or more

© 1997–2026 Citrix Systems, Inc. All rights reserved.

consecutive session requests are termed as Black hole machines. The reasons for these failures are related to various factors that might affect the machine, such as insufficient RDS licenses, intermittent networking issues, or instantaneous load on the machine. These failures do not include failures due to capacity or license availability. The presence of black hole machines in the environment increases session failures, resulting in poor session availability. The Black hole machines insights show the number of black hole machines identified in your environment.



Recommended actions for Black hole machines:

- Check RDS license on the machine
- Put the machine in maintenance mode
- Reboot

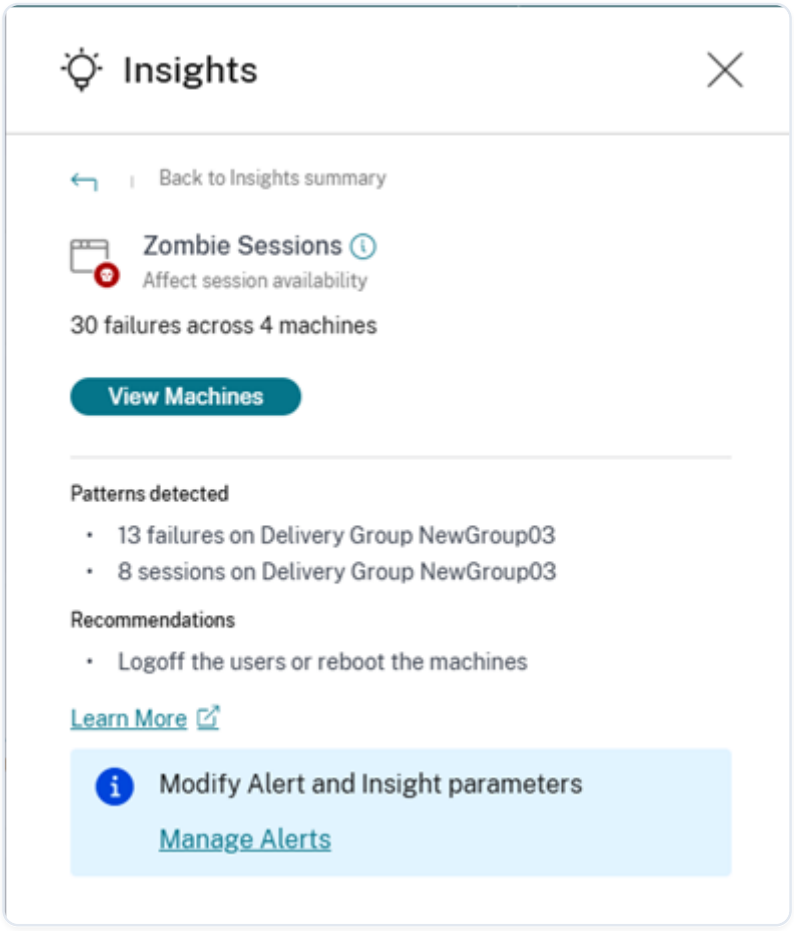
The Patterns Detected section shows the top patterns noticed in black hole machines with respect to the following criteria:

- Number of black hole machines running single-session or multi-session OS
- Delivery Group with highest number of impacted machines

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zombie Sessions

The Zombie Sessions sub-pane shows information on session failures that have occurred due to zombie sessions in the environment. A zombie session is an abandoned session on a single-session OS machine resulting in new session launches on the machine to fail. Attempts to launch sessions on this machine fail with an “Unavailable Capacity” error. All future session launch attempts fail until the abandoned session is terminated. Zombie session insights aim to help spot these machines with abandoned sessions and to proactively mitigate these failures.



Recommended actions for Zombie Sessions:

- You can log the users out of the Zombie sessions using Monitor for Citrix DaaS sites.
- You can reboot the machines containing Zombie sessions.

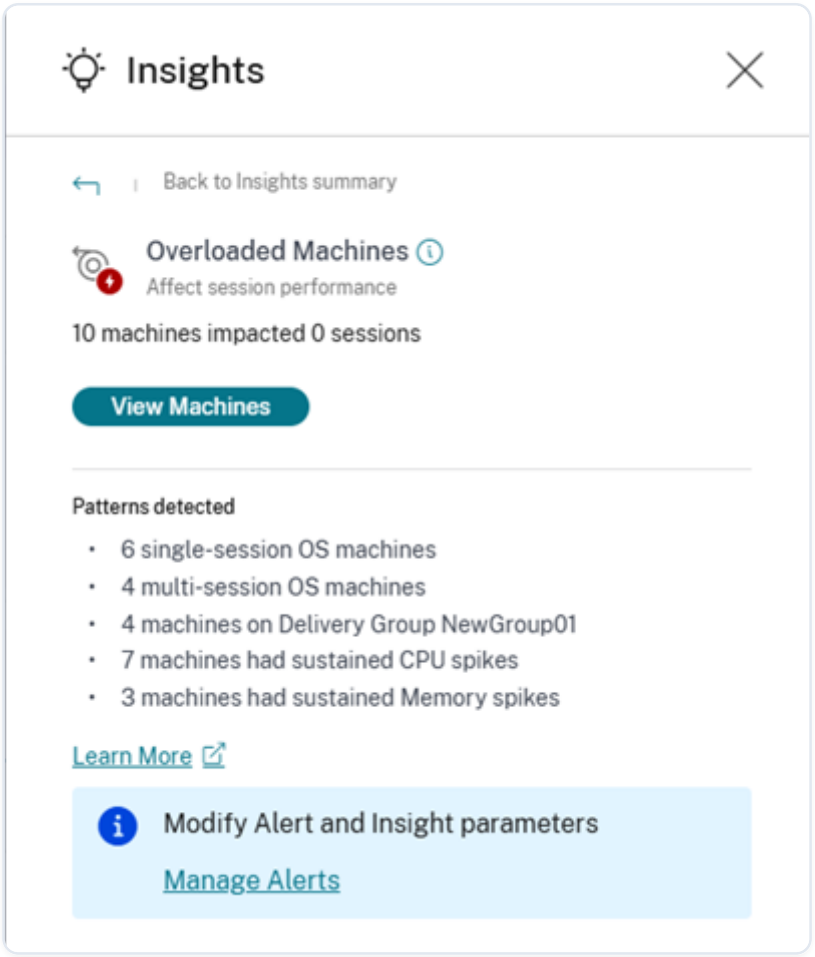
The Patterns detected section shows the top patterns noticed in Zombie sessions with respect to the following criteria:

- Delivery Group with highest number of impacted machines
- Delivery Group with highest number of impacted sessions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overloaded Machines

Overloaded Machines Insight gives visibility into overloaded resources causing poor experience. Machines that have experienced sustained CPU spikes, or high memory usage, or both, that have lasted for 5 minutes or more, that may result in a poor user experience are considered to be overloaded.



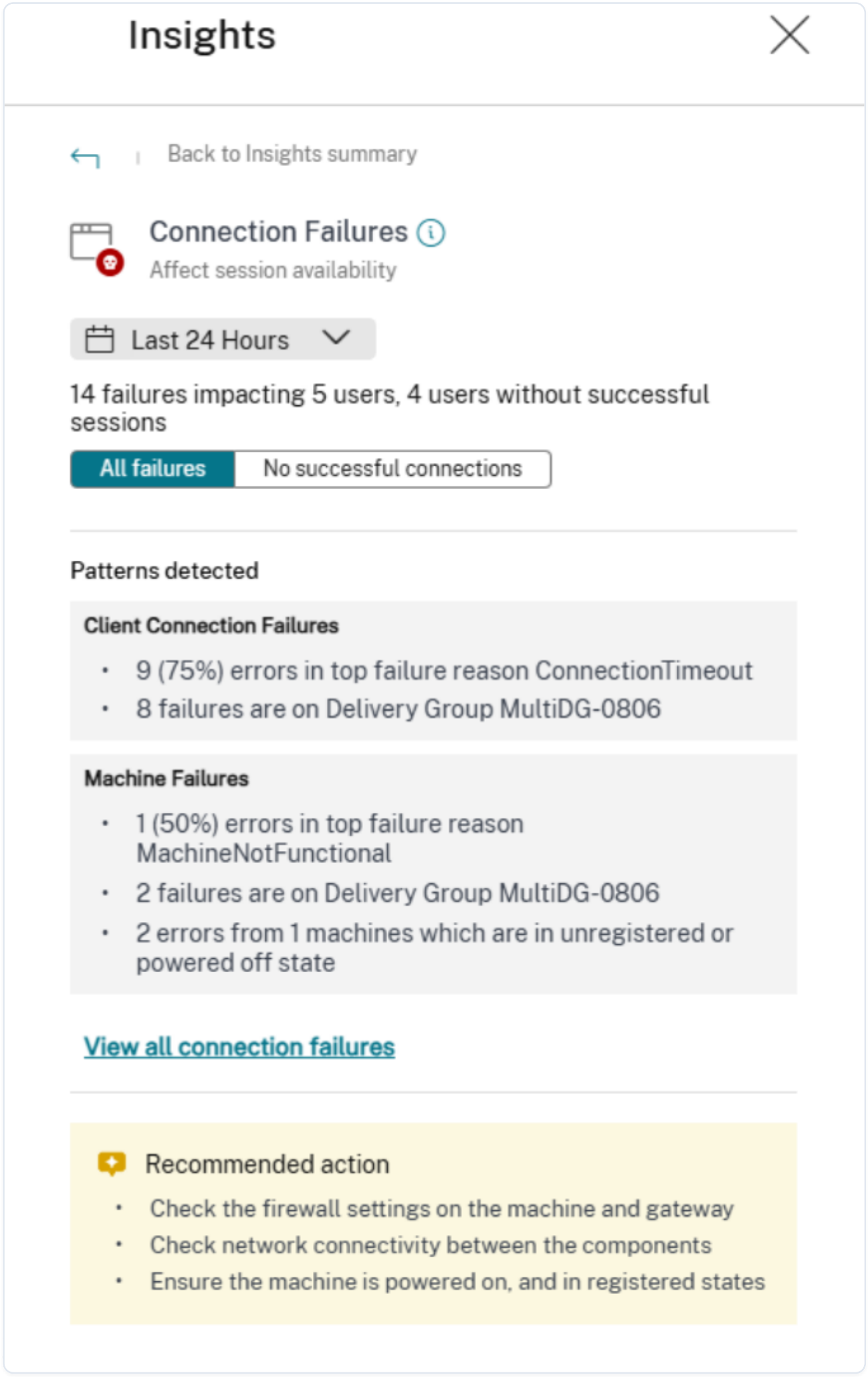
The Patterns Detected section shows the top patterns noticed in overloaded machines with respect to the following criteria:

- Number of overloaded machines running single-session or multi-session OS
- Delivery Group with highest number of impacted machines
- Number of overloaded machines with Sustained Memory or CPU spikes

Connection failures

The Connection Failures insight lists the number of session failures due to issues from the endpoint (where the user launches the session) until the machine (where the session is brokered). These failures can occur due to a variety of reasons, from incorrect firewall configurations, network communication issues, or machine unavailability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Insights
Back to Insights summary
Connection Failures
Affect session availability
Last 24 Hours
14 failures impacting 5 users, 4 users without successful sessions
All failures
No successful connections
Patterns detected
Client Connection Failures
9 (75%) errors in top failure reason ConnectionTimeout
8 failures are on Delivery Group MultiDG-0806
Machine Failures
1 (50%) errors in top failure reason MachineNotFunctional
2 failures are on Delivery Group MultiDG-0806
2 errors from 1 machines which are in unregistered or powered off state
View all connection failures
Recommended action
Check the firewall settings on the machine and gateway
Check network connectivity between the components
Ensure the machine is powered on, and in registered states

The two categories of connection failure categories are:

- Client connection failures —lists the sessions where communication errors have occurred on the endpoint.
- Machine failures —lists the sessions where errors have occurred at the machine.

Additionally, the Connection failures subpanel displays the following recommendations to resolve the errors.

- Check the firewall settings on the machine and the gateway.
- Check network connectivity between the components.
- Ensure machines are powered on, and in registered states.

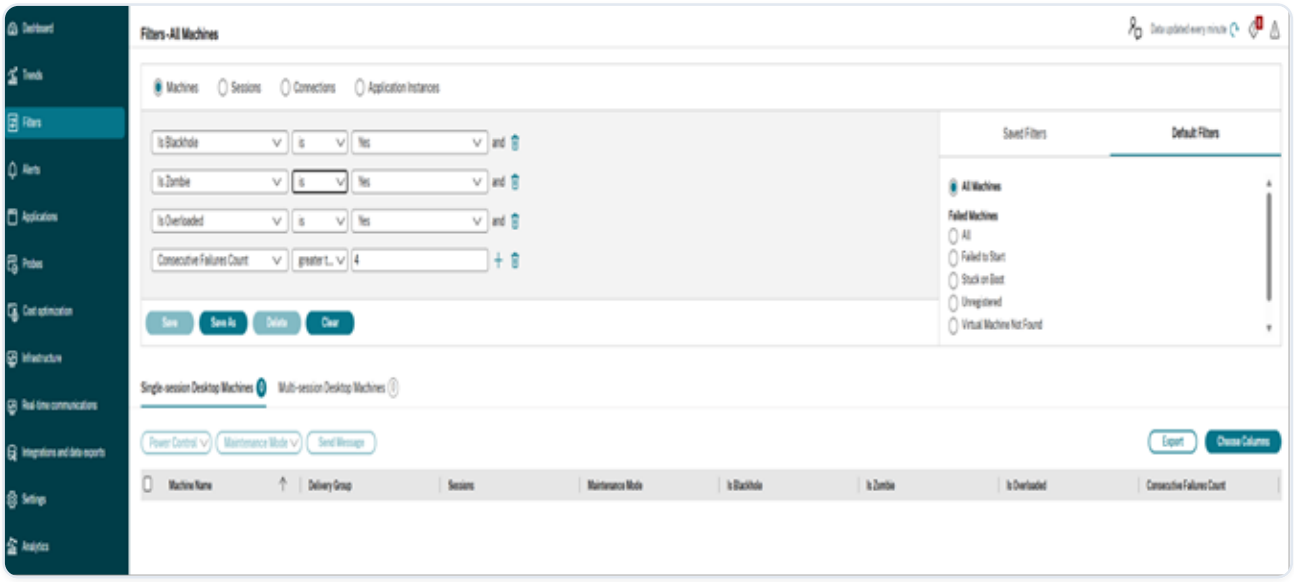
The failures are grouped to identify blocked users, i.e. users who have not had any successful sessions after their connection failure in the selected time duration. The patterns are highlighted for both categories of failures. Clicking the details opens the Connections view that is filtered to show all the sessions that have failed due to the errors in your environment during the selected time. This view helps analyze the individual sessions that have failed and get a possible root cause.

Filter View

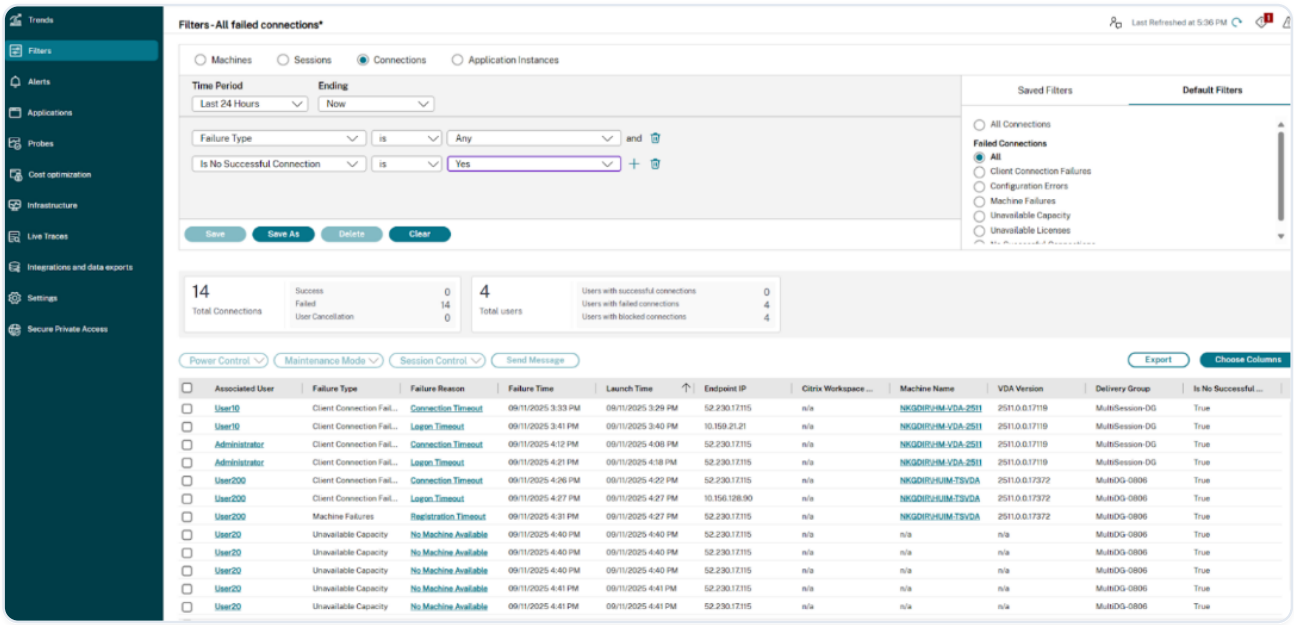
Following are new filters and columns that are added to Machines view under Filters -> Machines:

- Consecutive Failures Count: Number of consecutive session launch failures machine has reported
- Is Blackhole: Whether the machine has been identified as a black hole machine
- Is Zombie: Whether the machine has been identified as a zombie machine
- Is Overloaded: Whether the machine has been identified as an overloaded machine

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Following are new filters and columns that are added to Connections view under Filters -> Connections:



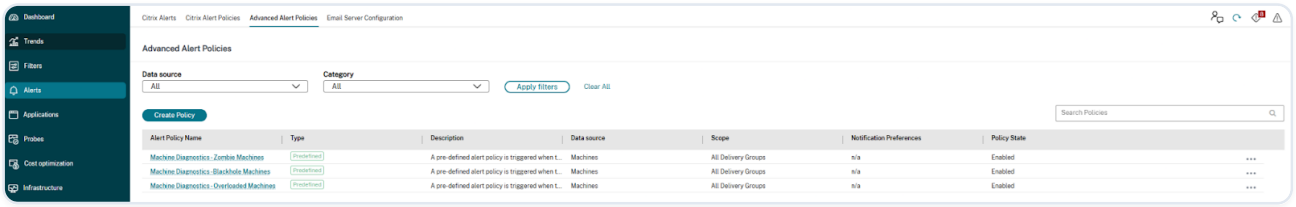
Alerts

There are 3 new “Advanced Alert Policies” that are available and enabled by default to help admins by proactively raising alerts in case Black hole, Zombie or Overloaded machines (across all delivery groups) are identified in the system

NOTE:

Connection failures are not supported under Advanced Alert Policies in the current release.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Managing Default Policies

To maximize the value of Diagnostic Insights, here are a few key points regarding the default alert policies:

- **Customization:** Administrators can customize the **alert policy parameters, scope, or notification actions** for these default policies.
- **Restrictions:** You **cannot change the conditions** or **delete** the default policies.
- **Enabling/Disabling:** Policies can be **disabled or enabled** as needed.
- **Notifications:** The default policies **do not have notifications configured** out of the box; they will only result in **UI alerts**. **We strongly advise administrators to update notification preferences** on these policies.

NOTE:

- The Insights Panel itself relies on enabled policies. If you disable the default policies and have no enabled custom policies, the Insights Panel will stop refreshing.
- Updating alert parameters also alter the calculation of the corresponding insight on the dashboard.

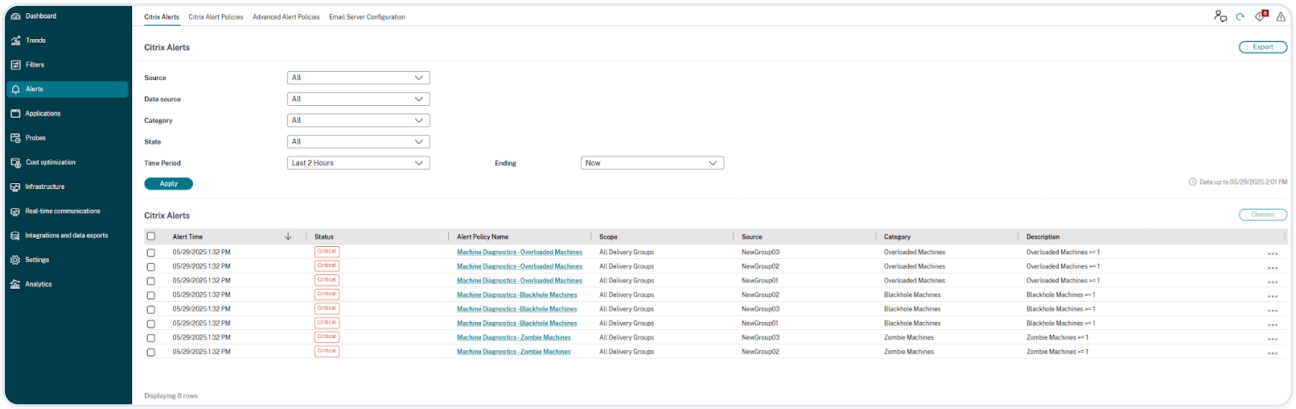
Creating Custom Policies

You can create additional **custom policies** for these insights. If you create a custom policy, we recommend **modifying the scope of the default policy** to **exclude any Delivery Groups** covered by your custom policy. This prevents overlap and potential duplicate alerts.

Alert notifications

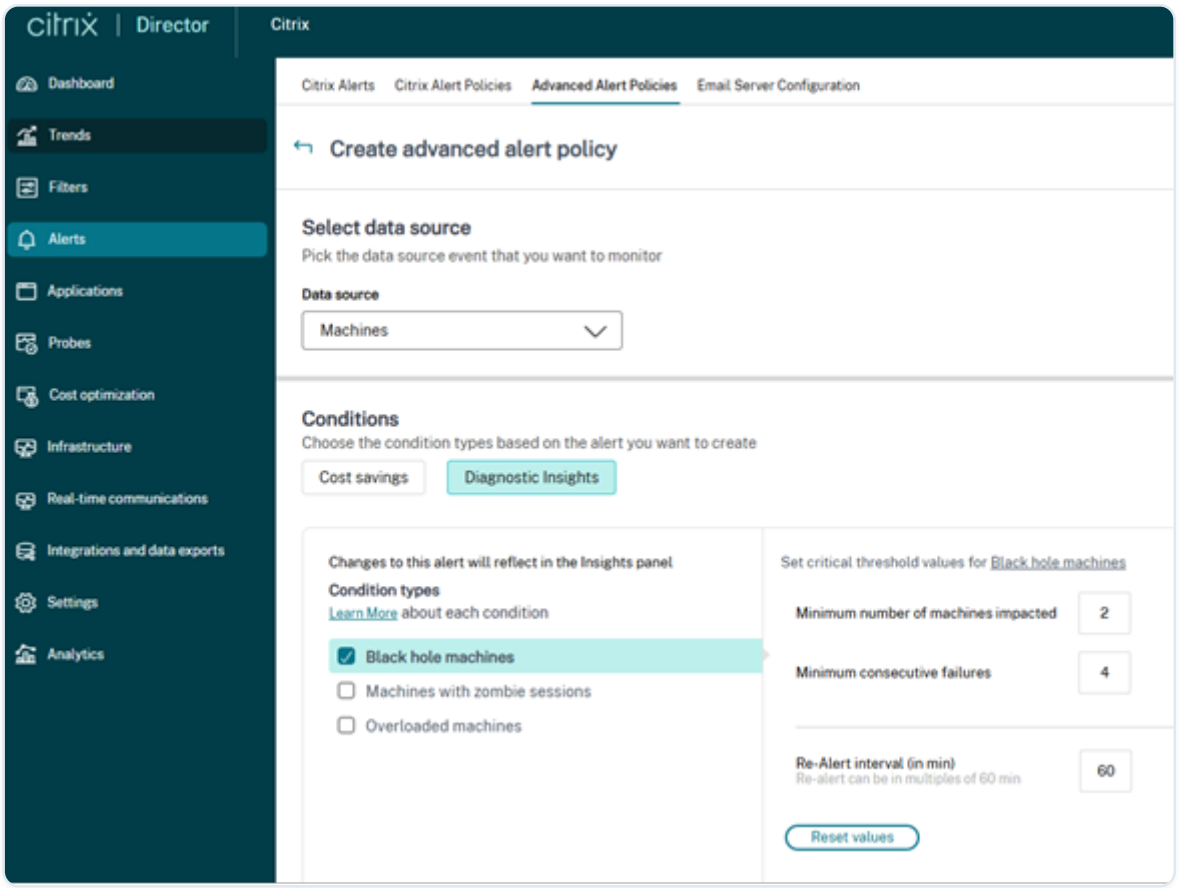
Following is a quick view of the ‘Citrix Alerts’ raised for the insights:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Alert for Black Hole Machines

Monitor scans for Black hole machines every 15 minutes and sends an alert to administrators to proactively mitigate session failures faced by users. Machines that have failed to service four or more consecutive session requests are termed as Black hole machines by default. The alert conditions and re-alert intervals can be customized for the selected alert.



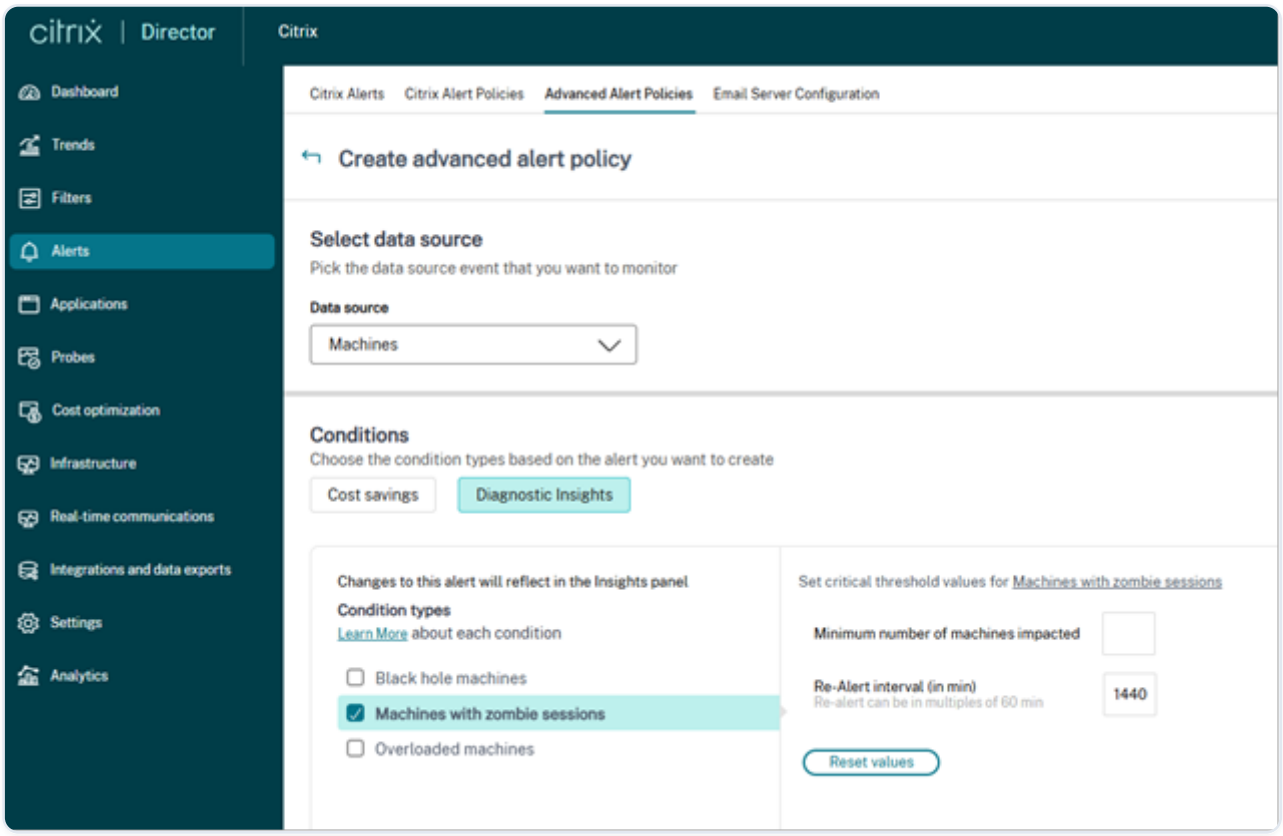
Details of the machines that caused session failures are sent in the alert emails or webhook payload. The Black hole machines alert policy must be enabled to receive these notifications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alert for Machines with Zombie Sessions

The Machines with Zombie Sessions alert is generated when a new machine with a zombie session is detected in the environment in a 15 mins interval.

Admins can customize the alert conditions for the Machines with Zombie Sessions alert.



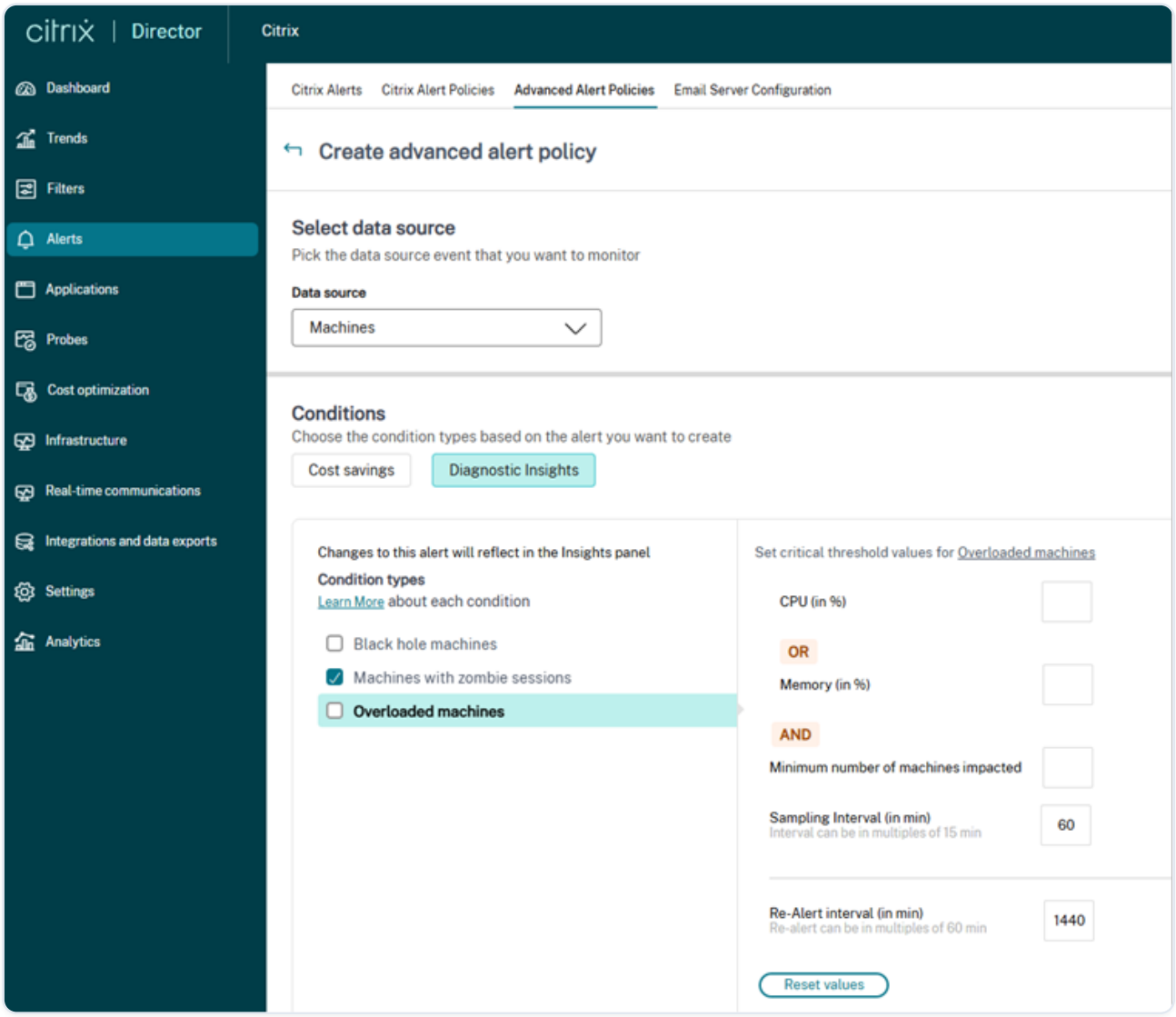
Details of the machines that caused the Zombie sessions and failures are sent in the alert emails or webhook payload.

Alert for Overloaded Machines

Machines that have experienced sustained CPU spikes, or high memory usage, or both for configured sampling intervals are considered to be overloaded.

Admins can customize the alert conditions and the re-alert preference for the Overloaded Machines alert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Re-alerts

For the specific insight alerts, the notification behavior within the configured **Re-Alert interval** is incremental. If new problematic machines are identified during this interval, the re-alert email or webhook will **only contain those new machines**. A full alert, listing all problematic machines for a given Delivery Group, will be sent once every **Re-Alert interval** (which is **24 hours by default**).

Geo Map visualization

Overview

The Map view in Citrix Director provides administrators with a comprehensive geographical visualization of successful session launches across their Citrix environment. This feature visually maps user connections on a global scale, helping IT teams quickly identify regional performance patterns, troubleshoot geographical connectivity issues, and optimize the end-user experience

© 1997–2026 Citrix Systems, Inc. All rights reserved.

based on location data. The map displays color-coded connection points that indicate logon performance across different geographical locations.

Prerequisites

The following table lists the features, endpoint metrics, and the supported product versions:

VDAs

VDA WINDOWS VERSION	VDA MAC VERSION	VDA LINUX VERSION
2411 or later	NA	NA

VIRTUAL DELIVERY AGENT VERSION	CITRIX WORKSPACE APP FOR WINDOWS VERSION	CITRIX WORKSPACE APP FOR MAC VERSION	CITRIX WORKSPACE APP FOR LINUX VERSION	CITRIX WORKSPACE APP FOR HTML5 VERSION	CITRIX WORKSPACE APP FOR CHROMEOS VERSION
2411 or later	2409 or later	2409 or later	2408 or later	2411 or later	2411 or later

NOTE:

The studio policy 'Endpoint Location Data Collection' must be enabled to access and display location data on the map. Please ensure this policy is configured before proceeding.

Key benefits

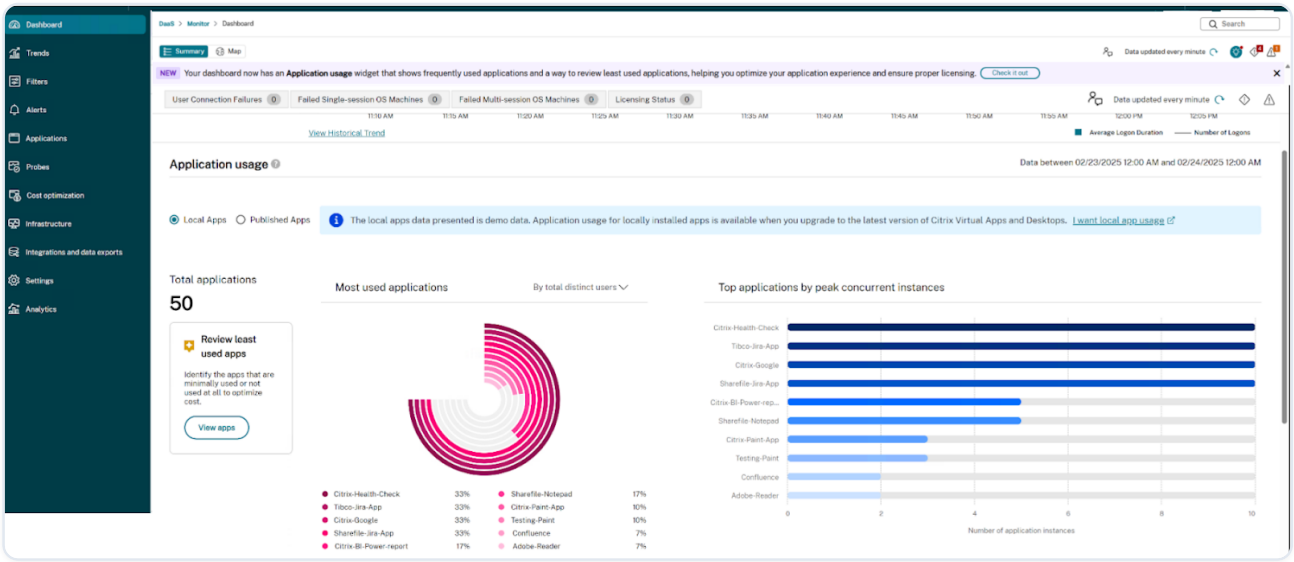
- **Geographical performance insights:** Instantly visualize connection performance metrics across different countries and regions.
- **Customizable performance thresholds:** Define your own standards for low, medium, and high (poor) logon durations.
- **Connection density visualization:** Identify high-traffic geographical areas through color-coded indicators and varying circle sizes.
- **Global deployment overview:** Access critical summary metrics for your entire environment.
- **Regional troubleshooting:** Quickly identify and address performance issues by geographical area.
- **Real-time monitoring:** View data that updates automatically every 5 minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

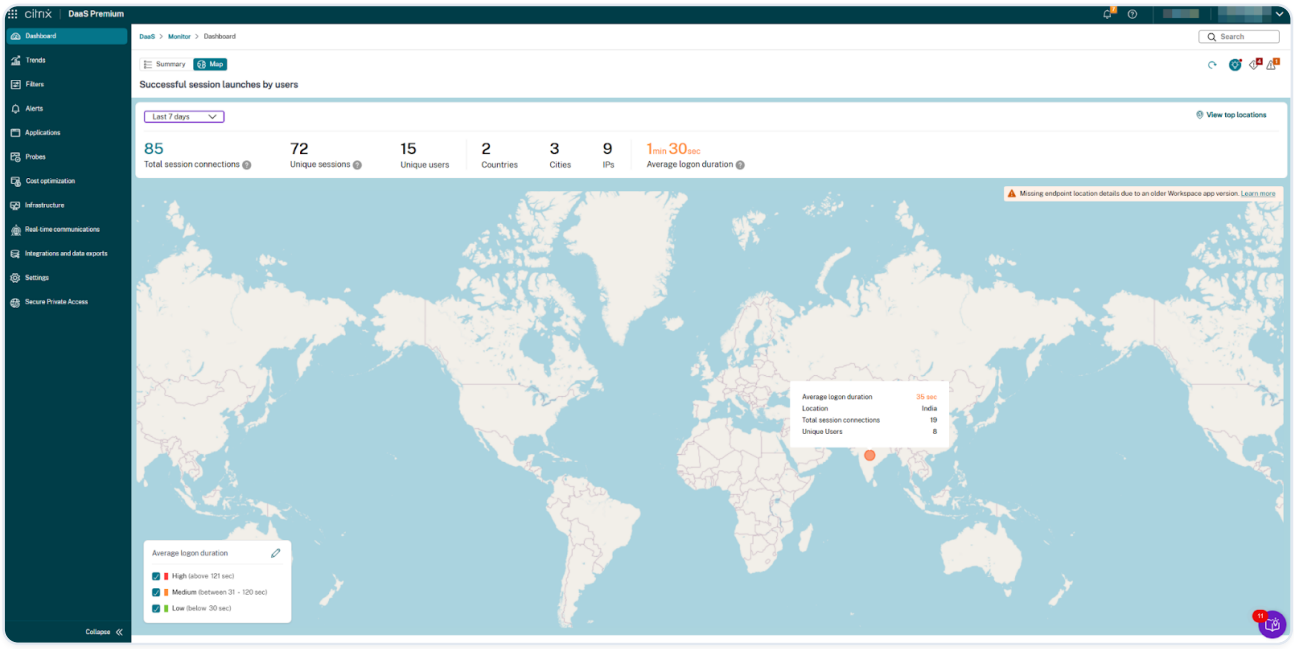
With full administrator permission, when you open Director, the Dashboard provides a centralized location to monitor the health and usage of a site.

The Dashboard contains Summary and Map views:

Summary view:



Map view:



User interface components

Navigation and view options

- **Summary/Map toggle:** Switch between summary statistics and geographical map visualization
- **Time range selector:** Filter data by time period (default: "Last hour")

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **View top locations:** Option to focus on areas with highest connection density
- **Data update indicator:** Shows when data was last refreshed (updates every 5 minutes)
- **Notification icons:** System alerts and messages related to the deployment

Summary dashboard metrics

At the top of the Map view, administrators can view the following critical deployment-wide metrics:

METRICS	DESCRIPTION
Total Session Connections	The aggregate number of session connections across all locations
Unique Sessions	The number of individual sessions established, excluding duplicates
Unique Users	The total count of distinct users who established connections
Countries	The number of different countries from which connections originated
Cities	The number of distinct cities from which connections originated
IPs	The total number of unique IP addresses that established connections
Average Logon Duration	The mean time taken for session establishment across the entire deployment

Performance classification

Connection performance is categorized into the following three tiers, with customizable thresholds:

PERFORMANCE LEVEL	COLOR CODE	DEFAULT THRESHOLD	DESCRIPTION
Low (Good)	Green	Below 60 sec	Fast logon experiences with minimal delays

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PERFORMANCE LEVEL	COLOR CODE	DEFAULT THRESHOLD	DESCRIPTION
Medium	Orange	61-120 sec*	Acceptable logon times
High (Poor)	Red	Above 120 sec	Suboptimal logon experiences requiring attention

NOTE:

The interface allows administrators to customize these thresholds through input fields in the legend panel.

Map legend and threshold controls

The interactive legend panel provides:

- **Color-coded performance indicators** with corresponding threshold values
- **Editable threshold fields** for customizing Medium performance range (minimum and maximum values)
- **Validation message** ensuring the maximum threshold exceeds the minimum threshold and is neither zero nor negative
- **Selection/filter controls** to focus on specific performance categories

System requirements and notifications

Citrix Workspace app version compatibility

The map displays a warning banner when endpoint location details are missing due to outdated Citrix Workspace app versions:

- **Warning message:** "Missing endpoint location details due to an older Workspace app version."
- **Resolution:** Upgrading to the latest Workspace app version ensures complete geographical data collection
- **Learn more:** The banner includes a link to documentation with additional information on version requirements

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration options

Setting performance thresholds

- Locate the legend panel on the bottom left of the Map view.
- Enter custom values for Medium performance category:
  - Minimum threshold (default: 61 sec)
  - Maximum threshold (default: 120 sec)
  - The Low category automatically adjusts to "below ".
  - The High category automatically adjusts to "above ".
  - Validation ensures maximum threshold exceeds minimum threshold and neither is zero or negative.
  - Changed threshold values are stored in browser cache (local storage) and are specific to the browser.

Time range configuration

1. Use the dropdown menu in the top-left corner of the metrics section.
2. Select the desired time period (default: "Last hour").

The map and metrics automatically update to reflect data from the selected period.

Map view usage

You can use the Map view for the following:

Regional performance troubleshooting

1. Identify regions showing predominantly red (High) logon duration indicators.
2. Correlate with infrastructure components serving those regions.
3. Implement targeted optimizations for affected geographical areas.

Capacity planning

1. Review connection density patterns by observing circle sizes across different regions.
2. Identify high-traffic geographical areas (larger circles) requiring additional resources.
3. Plan infrastructure scaling based on regional usage patterns.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Global deployment assessment

1. Use the metrics panel to understand the scale of your deployment (total connections, unique users).
2. Compare logon performance across different geographical regions.
3. Establish baseline performance expectations for different locations.

Threshold optimization

1. Review the distribution of green, orange, and red indicators across the map.
2. Adjust thresholds to better reflect acceptable performance for your specific environment.
3. Create more meaningful performance categorization based on actual user experience.

Troubleshooting

Missing geographical data

If the warning banner "Missing endpoint location details due to an older Workspace app version" appears:

1. Identify users with outdated Citrix Workspace app versions.
2. Plan a phased upgrade to the latest Citrix Workspace app version.
3. Prioritize upgrades in regions where geographical data is most critical.

Performance categorization issues

If performance categories seem inaccurately represented:

1. Review current threshold settings in the legend panel
2. Adjust the Medium category minimum and maximum values as needed
3. Ensure thresholds align with your environment's actual performance characteristics and expectations

Data refresh issues

If data seems outdated:

1. Check the Data updated every 5 minutes indicator for the last refresh time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For the past week, auto-refresh is disabled. Refresh manually to get the latest data.

1. Verify the selected time range matches your troubleshooting period.
2. Use the Refresh button if available to manually update the data.

Best practices

- Regularly review and adjust performance thresholds based on infrastructure improvements.
- Use the **View top locations** option to focus on areas with the highest connection volume.
- Compare geographical performance patterns before and after infrastructure changes.
- Create baseline reports of regional performance during optimal operation periods.
- Consider regional network conditions when setting performance expectations.
- Educate users about upgrading to the latest Citrix Workspace app version for complete data collection.
- Regularly check the **Map View** to identify emerging trends in session performance.

deviceTRUST® integration in Monitor

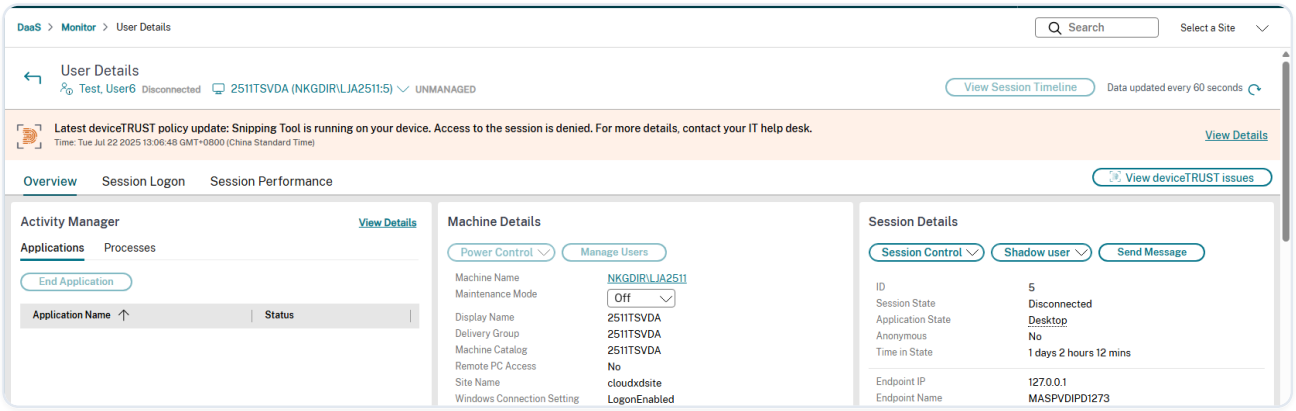
The deviceTRUST® integration brings contextual security information directly into Monitor. This feature is visible only when the deviceTRUST components are installed and configured in your Citrix Virtual Apps and Desktops™ environment.

deviceTRUST continuously monitors the device context and ensures that remote devices connecting to your Citrix environment meet your organization's security policies. If a device falls out of compliance, deviceTRUST can automatically take action, such as disconnecting or signing out the session.

Highlighted session interruptions on the User Details page

Sessions that have been interrupted or terminated by a deviceTRUST action are highlighted on the **User Details** page. This indicates that the disconnection was a deliberate security measure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

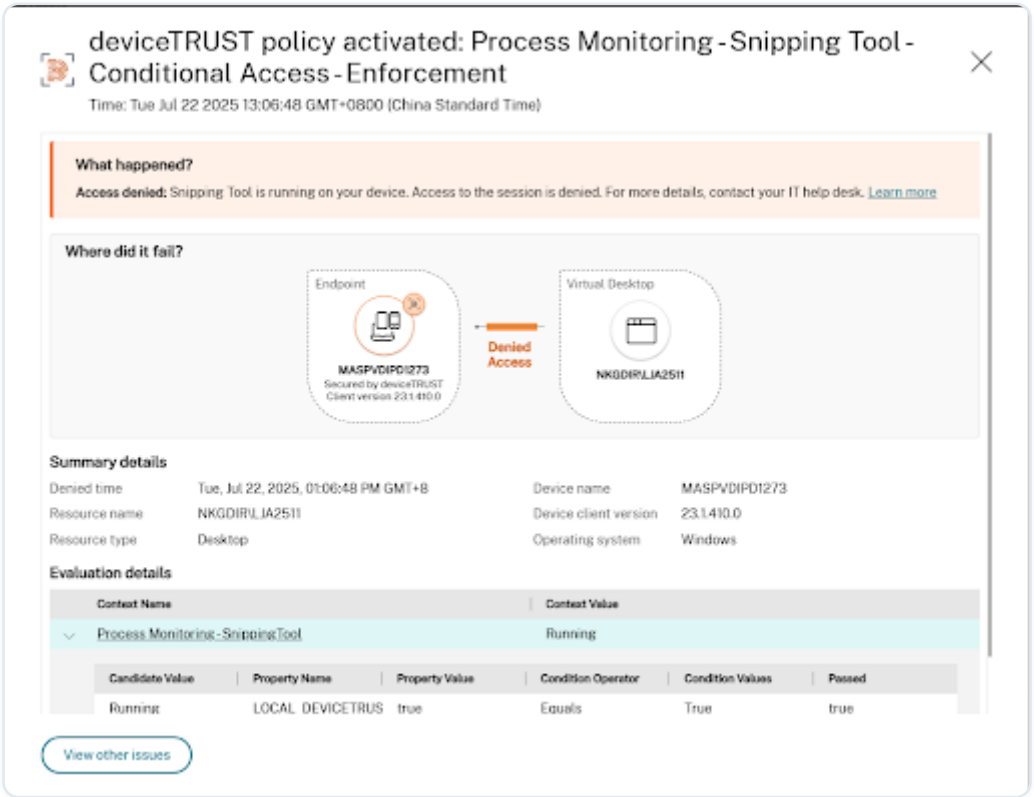


View deviceTRUST issues button on the User Details page

A **View deviceTRUST issues** button is available on the **User Details** page. Clicking this button takes the admin to the **Denied Access** tab if there are deviceTRUST issues for the session in the last two days. The button appears greyed out if there are no deviceTRUST issues for the session in the last two days.

Detailed deviceTRUST failure information

Admins can view the exact reason for an access denial due to deviceTRUST issues by clicking **View Details** from the highlighted issue banner. The following details are displayed:



- The reason for the access denial.

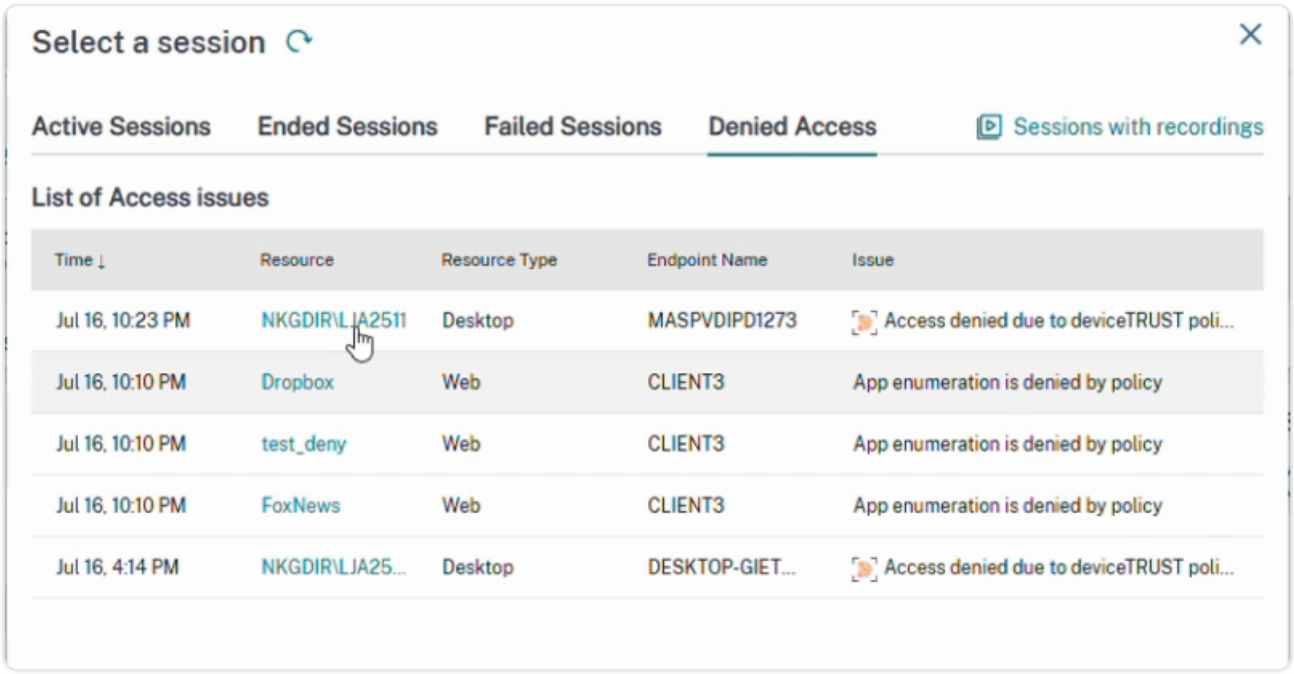
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A visual representation of where the connection was blocked between the user's endpoint device and the virtual desktop.
- Summary details of the access denial, including the time the issue occurred, resource name, resource type, the device from which the connection attempt was made, and the deviceTRUST client version.
- Policy evaluation details, including the properties and conditions that were not met.

Click **View other issues** to navigate to the **Denied Access** tab.

Updated Denied Access tab

The **Denied Access** tab has been updated to include deviceTRUST issues. This tab provides a historical list of all denied accesses from deviceTRUST and Secure Private Access. Admins can view detailed deviceTRUST failure information by clicking a deviceTRUST item.



Session Score

Prerequisites

Session score via uberAgent lite is available from VDA version 2511 or later. The capability is also being backported to LTSR 2507 via CU2.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

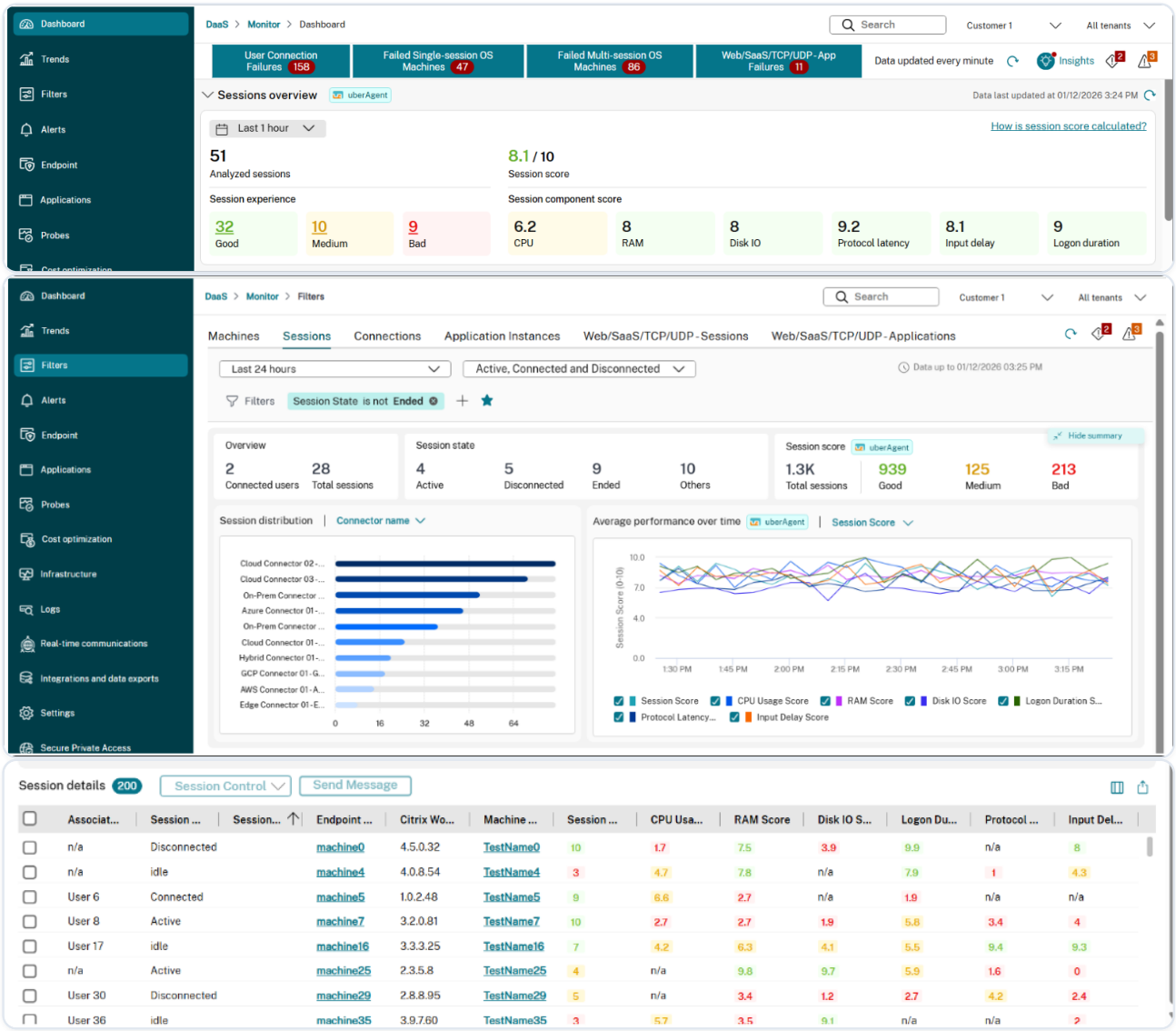
Overview

Session details now contain additional data-points to troubleshoot session performance and analyse overall session health. The additional data provides insights into the overall user-experience of individual sessions and help Admins understand the reason for poorly performing sessions.

1. Session experience summary – It serves as a quick peek into the session experience. Shows the summary of user-experience across all the launched sessions within the environment during the selected time-period. Analysed sessions are categorised into Good, Medium, and Bad. Admins can click on an experience category to open the detailed session view (Filters page) with automatically applied filters.
2. Session and component score – Session summary also provides the average session and component score for the analysed session. While standalone average scores maybe not be a very useful metric, it can still serve as a good indicator of the session experience for majority sessions. Similarly, Admin can use the average component scores to understand the potential root cause of Bad sessions.
3. Session distribution – Session distribution chart is added on the filters page. Admin can view the session distribution by Endpoint Country, City, Endpoint OS, CWA version, ISP, etc.
4. Performance trends – Session performance trends chart is also added on the filters page. Performance chart is helpful for analysing the session and component performance trends and identify any recurring patterns based on time of day, country, etc.
5. Individual session data – Following data points have been added for each session in the Session details table –
    a. Session score
    b. CPU score
    c. RAM score
    d. Disk IO score
    e. Protocol Latency score
    f. Input delay score
    g. Logon duration score

For more information about experience score calculation, see Experience Score.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Endpoint OS Version Visibility

The **Session** and **Connection** pages include an **Endpoint OS Version** column and a corresponding filter. The column lets you view the endpoint operating system version. You can filter sessions or connections based on the OS version from which the user launches. This feature supports Windows and Linux devices.

Advantages

- View the endpoint OS version on both the **Session** and **Connection** pages.
- Filter sessions or connections based on the endpoint OS version.

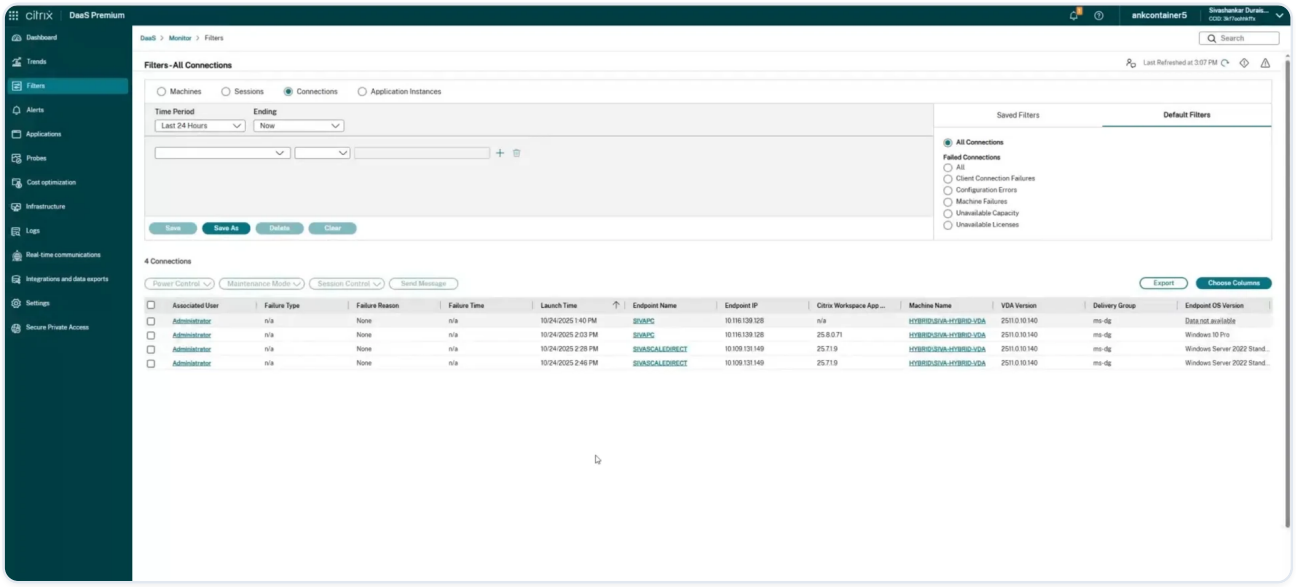
Example usage

To filter sessions or connections launched from a specific Windows OS version:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to the **Sessions** or **Connections** page.
2. Locate the filter for the **Endpoint OS Version** column.
3. Enter the specific text for the Windows version you want to filter by (for example, `Windows 10`).
4. Apply the filter.

Example: If you enter `Windows 10` in the filter, the list updates to show only connections or sessions launched from Windows 10 machines.



Applicability

- Windows devices
- Linux devices

System requirements

- **Minimum App Version:**
  - Windows CWA App version: 2508
  - Linux CWA App version: CWAL 2601
- **Minimum VDA Version:** VDA version 2511

Limitations

- The **Endpoint OS Version** column displays values only for Windows and Linux devices. Other operating systems are not currently supported. Support for other operating systems is planned for future releases.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Endpoint Security Policy activation & threat detection reporting

Citrix Workspace App is introducing built-in security checks that will automatically detect high-risk conditions, such as Microsoft Recall enabled on endpoints without the need for any manual configuration. This real-time visibility of such detections will be available in Citrix Monitor and Monitor. The reporting will enable the administrators to quickly assess the risk and configure their protection policies to ensure a safer environment. While detection for select events like Recall is automatic, protection from events requires manual configuration of app protection policies by the admin. Activation events for all enabled policies will also be reported in Monitor and Monitor. By utilizing proactive risk management and policy reconfiguration, Admins will be able to strengthen endpoint security in their environment and reduce exposure to emerging threats.

The following reporting will be available in Monitor:

- **Audit Trail**
    - **Automatic Detection** – During its default scan, CWA detects various threats like Windows Recall on the endpoint. If a threat is detected, CWA will send an event to Monitor. The following data will be reported for each event –
        - Timestamp
        - Username
        - Endpoint name
        - Endpoint OS
        - CWA version
        - Event name
        - Event type – Detection or protection
- **Protection for configured policies** – Administrators can configure protection policies to prevent certain events such as Screen capture, DLL injection, or Keylogging. Anti screen capture policy can be used to prevent screen capture attempts by recall as well. Protection events reported in Monitor will include all the data points listed above.
- **Aggregated insights and trends** – Events data will be aggregated to report the following information:
    - Detection/protection summary for the environment,
    - Top protected/detected events, and
    - Trend of protection and detections events over time

© 1997–2026 Citrix Systems, Inc. All rights reserved.

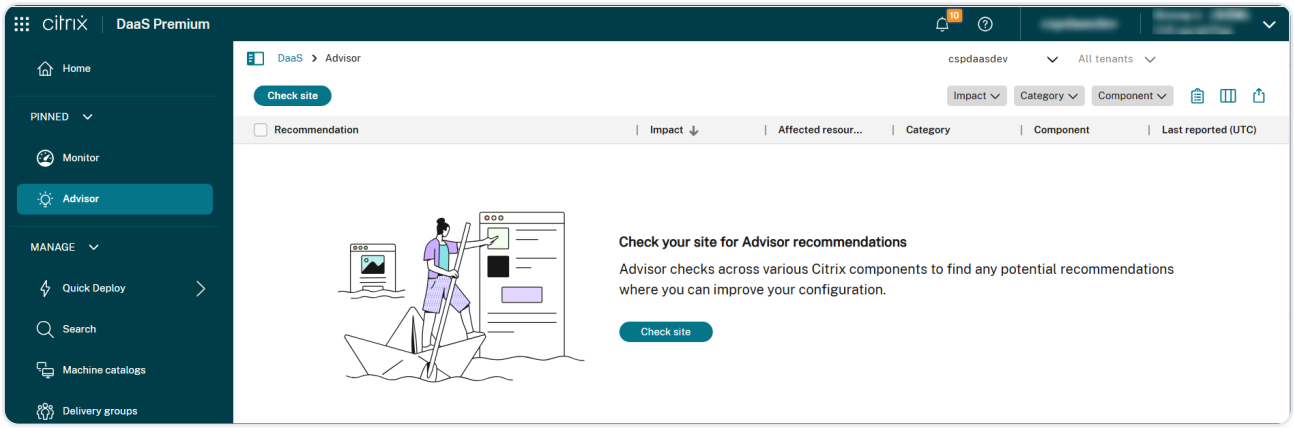
This capability is designed to further strengthen Citrix's commitment to securely deliver applications by helping organizations identify emerging threats and respond to them in real time.

Administrators can use the above insights to better understand the security "threats" in their environment and setup protection policies to protect sensitive data, minimize security risk, and support the establishment of related corporate level policies designed to mitigate such risk. (e.g. discourage the use of tools like recall, keylogger, etc.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Advisor

Citrix Advisor is a service that helps you optimize DaaS deployment and enhance its overall health and readiness. It automates environment checks and delivers actionable recommendations, empowering you to proactively identify configuration issues, inefficiencies, resource wastes, deviations from best practices, and more.



NOTE:

- This service is available exclusively to **Full Administrators**.
- We recommend submitting your feedback using the feedback icon in the top-right corner of the page.

Benefits

With Advisor, you can:

- **Proactively identify and resolve issues**: Detect potential problems, configuration drift, and deviations from best practices before they impact users, disrupt business operations, or compromise security.
- **Optimize environment performance and stability**: Fine-tune configurations, optimize resource allocation, and implement best practices to enhance the stability, security, and performance of your Citrix deployments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Streamline operations and reduce overhead**: Automate routine checks, simplify complex remediation tasks, and receive guided assistance, thus reducing operational overhead and freeing up administrative resources.
- **Optimize costs and resource utilization**: Identify areas of overspending, uncover opportunities for resource optimization, and ensure efficient utilization of Citrix technologies to minimize the total cost of ownership.
- **Maintain compliance and adherence to best practices**: Ensure that your Citrix deployments adhere to Citrix best practices, security standards, and industry regulations, reducing risk and improving overall governance.
- **Simplify complex tasks**: Simplify administrative tasks to support a healthy, optimized environment.

Check for recommendations

Advisor automatically runs site checks on a recurring weekly schedule (Sundays at 2:00 AM UTC), giving you a regularly updated view of your environment health. Each run generates a report retained for up to 90 days and then automatically purged. Recommendations from the most recent scheduled run appear on the **Advisor** page and in the **Advisor** widget on the **Home** page.

You can also run a site check manually at any time. A manual check updates recommendation immediately regardless of the scheduled run cycle.

To run a manual site check, follow these steps:

1. Sign in to Citrix Cloud using an account with the **Full Administrator** role.
2. Click the **DaaS** tile.
3. In the left pane, select **Advisor**.
4. Click **Check site**.
5. On the **Check site** page, select the categories you want Advisor to check.

CATEGORY	DESCRIPTION	REFERENCE
Security	Recommendations for detecting threats and vulnerabilities that might lead to security breaches.	Security recommendations

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	DESCRIPTION	REFERENCE
Reliability	Recommendations for ensuring and improving the continuity of your business-critical applications.	Reliability recommendations
Performance	Recommendations for enhancing performance across applications and desktops to deliver faster, more responsive experiences for end users.	Performance recommendations
Operational excellence	Recommendations for helping you achieve process and workflow efficiency, resource manageability, and deployment best practices.	Operational excellence recommendations
Cost optimization	Recommendations for reducing overall spending by right-sizing resources, minimizing waste, and aligning capacity with actual usage needs.	Cost optimization recommendations

6. Click **Run check** to run a site check and generate updated recommendations based on the current configuration.

   All recommendations appear in the list.

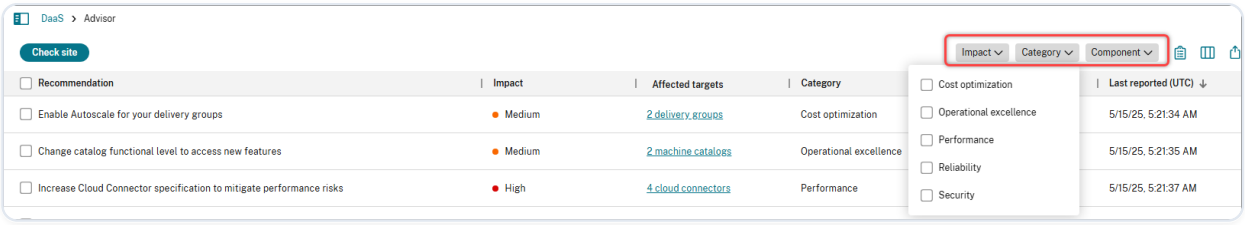


Filter recommendations

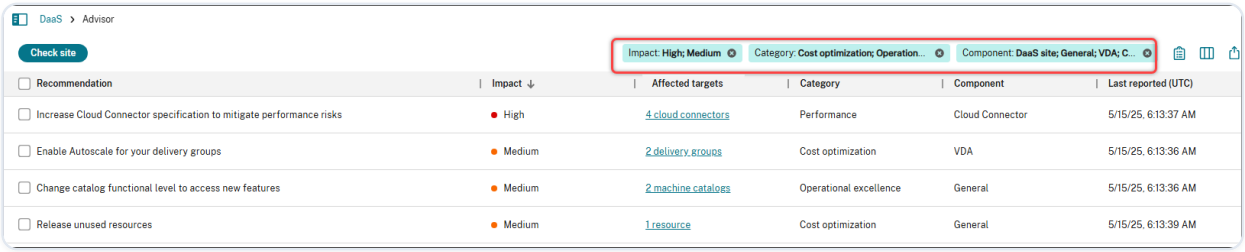
You can filter recommendations by **Impact**, **Category**, or **Component** to focus on the information most relevant to your deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In **Advisor**, locate the filters at the top right of the recommendation list.



2. Click a filter (for example, **Category**) to view available options.
3. Select one or more checkboxes to apply the filter. The list updates automatically to display only the recommendations that match your selections.
4. Use multiple filters together to narrow down the list.



Review and act on recommendations

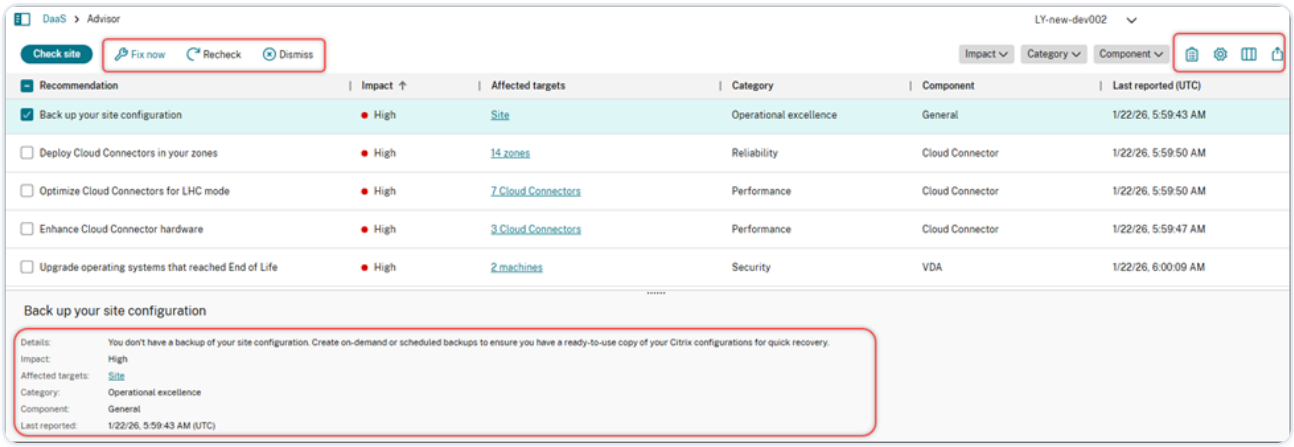
Use the recommendations list to understand configuration issues and improvement opportunities in your deployment. You can take the following actions on recommendations:

- View recommendation details
- Implement recommended actions
- Dismiss recommendations
- Dismiss specific affected targets in a recommendation
- Customize check rules
- View the full site check report

View recommendation details

To review a recommendation, select a recommendation to view its details in the lower pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

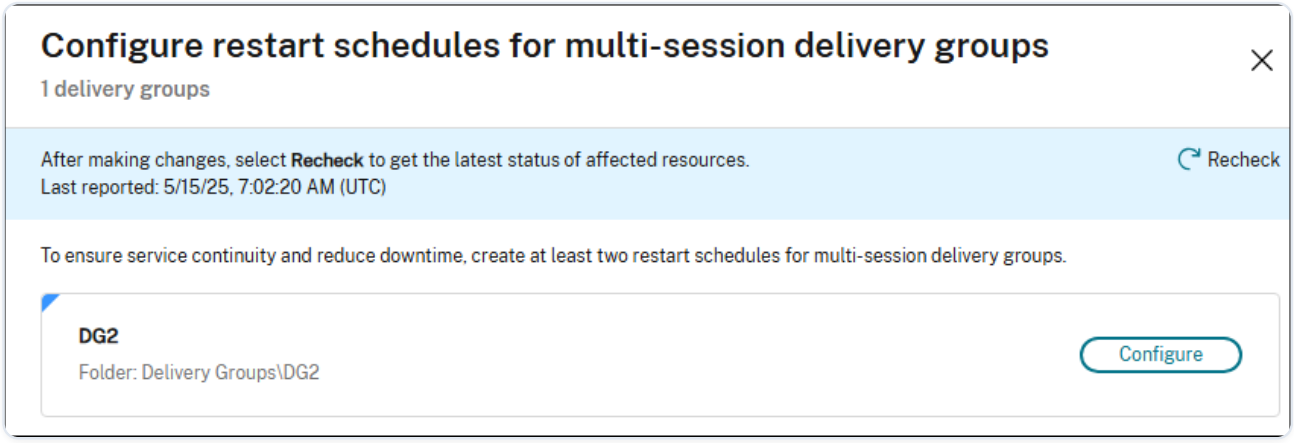


Implement recommended actions

To implement the recommended actions for a recommendation, follow these steps:

1. Select a recommendation.
2. Click **Fix now** in the action bar.
3. Follow the recommended steps to make the necessary updates.

   Sometimes, you're directed to supporting documentation when automated configuration isn't supported or feasible. We want to make sure that Advisor is designed to provide automated actions directly within the UI wherever possible, minimizing the need for manual setup.
4. After making updates, click **Recheck** to update the status of the affected targets.



NOTE:

The UI and steps vary depending on the recommendation. The screenshot shown is for illustration purposes only.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dismiss recommendations

If a recommendation isn't relevant to your deployment or doesn't require action, you can remove it from the current list and future check results:

1. Select the recommendation.
2. Click **Dismiss** in the action bar.

TIP:

To restore a dismissed target in a recommendation, click the **Gear** icon in the upper-right corner above the recommendation list, and select **Manage dismissed items**

Dismiss specific affected targets in a recommendation

If a recommendation includes affected targets that are intentionally non-compliant with best practices (*for example*, test, validation, or temporary resources), you can remove them from this recommendation (granular dismissal).

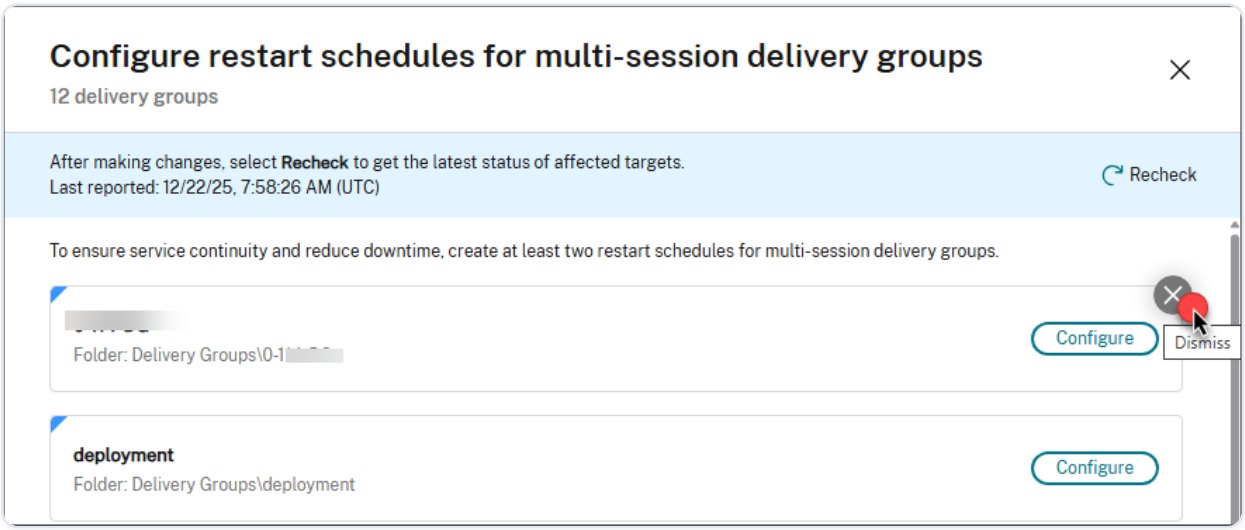
NOTE:

Granular dismissal is supported only for the following targets: machine catalogs, delivery groups, application groups, and zones.

Detailed steps are as follows:

1. Select the recommendation.
2. Click the **Affected targets** field of the recommendation. The recommendation page displays all affected targets.
3. Hover over the affected target that you want to dismiss. A **Dismiss** icon appears in the top-right corner of the target.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click the **Dismiss** icon. A dismissal confirmation dialog box appears.
5. Enter a note for the dismissal if needed, and then click **Dismiss**. The affected target is removed from the recommendation page.

TIP:

To restore a dismissed target in a recommendation, click the Gear icon in the upper-right corner above the recommendation list, and select **Manage dismissed items**.

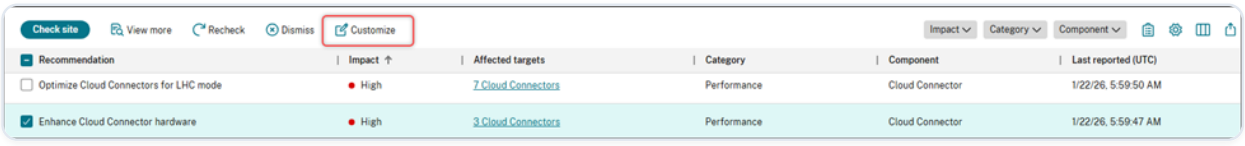
Customize check rules

You can customize Advisor check rules for the following recommendations:

- **Enhance Cloud Connector hardware:** Adjust thresholds for CPU, memory, and disk usage, and exclude specific disks.
- **Release unused resources:** Define custom unused time thresholds for machines and applications.
- **Optimize GPO configuration for VDAs:** Modify the GPO processing time threshold.

To customize the check rule for a single recommendation, follow these steps:

1. Select a recommendation and click **Customize** in the action bar.



2. On the **Customize** page, update the check settings as needed.
3. Click **Save**. Changes take effect the next time you run the check.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

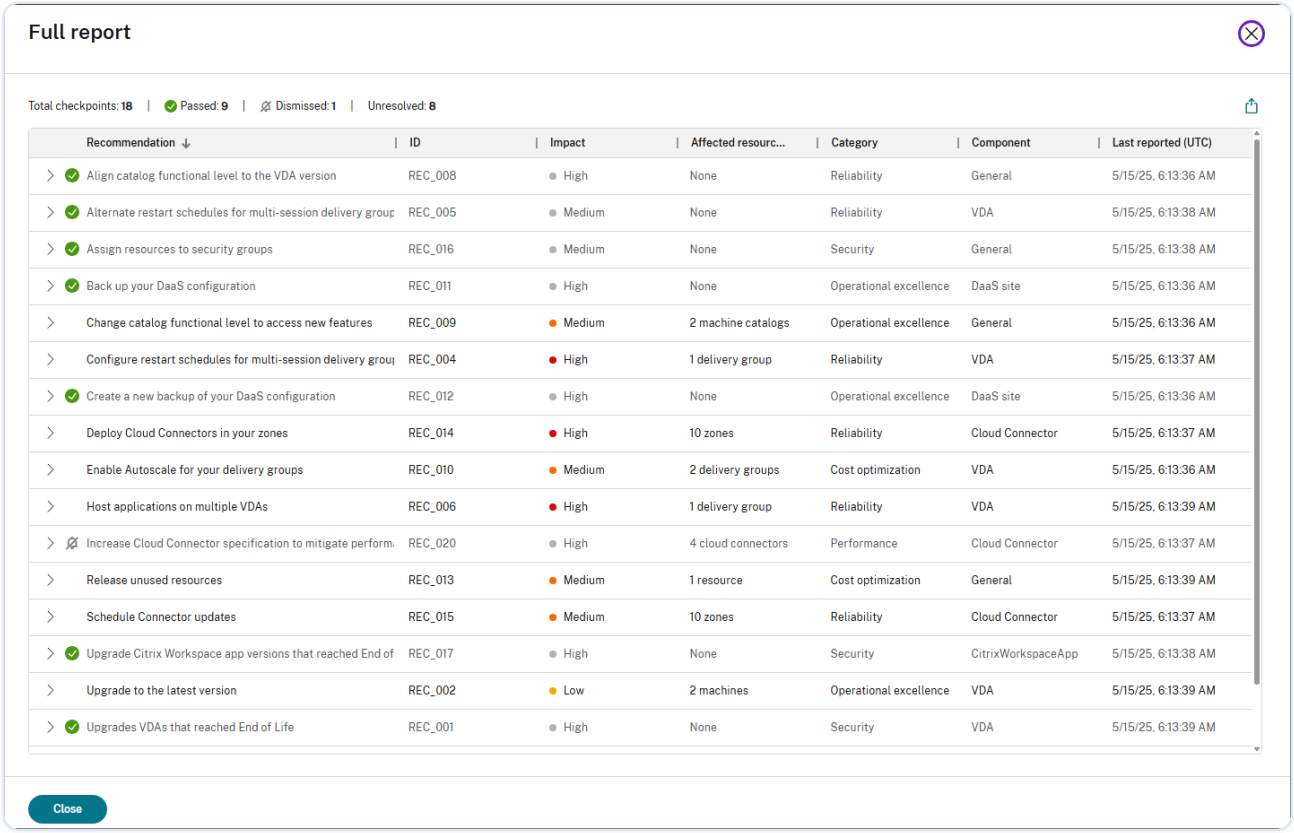
To customize check rules for all three recommendations from a central location, follow these steps:

1. Click the **Gear** icon in the upper-right corner above the recommendation list, and select **Customize rules**. The three recommendations appear.
2. Click the **Edit** icon next to a recommendation.
3. Update the check settings as needed.
4. To update check rules for the remaining recommendations, repeat steps 2–3.
5. Click **Save**. Changes take effect the next time you run the check.

View the full site check report

The **full report** provides a summary of all Advisor recommendations from the latest site check. It includes passed, dismissed, and unresolved checkpoints, helping you assess the overall health and optimization opportunities in your DaaS site.

To view the full report, click the **View full report** icon at the top right of the recommendation list.



Set up StoreFront for Advisor check

StoreFront-related recommendations in Citrix Advisor require additional setup. To set up StoreFront for Advisor checks, complete the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Add your StoreFront servers to Infrastructure Monitoring by creating corresponding connections. For more information, see Infrastructure Monitoring setup.
2. If you configure a StoreFront connection in **Manual connection** mode, ensure that Citrix Infrastructure Monitoring version 2603 or later is downloaded and installed. To verify a required version is installed:
   a. Go to **Monitor > Settings**.
   b. Locate the connection where **Type** equals `StoreFront`.
   c. Confirm that the **Version** field displays `7.47` or greater.

IMPORTANT:

After you apply changes to your StoreFront deployment based on Advisor recommendations, wait at least 6 hours before rechecking the same recommendations. This delay allows Infrastructure Monitoring to collect and process updated telemetry and ensures that Advisor evaluates the most current data.

References

This section lists all Citrix Advisor recommendations by category to help you understand their purpose and impact.

Security recommendations

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
Upgrade VDAs that reached End of Life	REC_001	High	VDA	Some machines are using VDA versions that have reached End of Life and are no longer supported by Citrix. Upgrade affected machines to the latest LTSR or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				CR VDA version.
Assign resources to security groups	REC_016	Medium	General	Some resources are assigned to individual users. It is a Citrix best practice only to assign user access through security groups to streamline management and enhance security. Reconfigure the user assignment for delivery and application groups to include only security groups.
Upgrade Citrix Workspace app versions that reached End of Life	REC_017	High	Workspace app	Some endpoint devices use a Citrix Workspace app version that reached End of Life. Upgrade devices to the latest Workspace app version to reduce supportability and security

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				risks. For simplified version management and automatic update control, use Global App Configuration Service. Additionally, consider using endpoint analysis solutions to enforce a minimum Workspace app version to access the store.
Implement device posture policies	REC_021	Medium	Secure Private Access	The current Secure Private Access configuration lacks device posture policies, allowing unrestricted access to internal applications from any device. To mitigate this risk and enhance security, implement

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				device posture policies that classify devices as: **Compliant**, **Non-compliant**, and **Denied access**.
Implement adaptive access policies	REC_022	Medium	Secure Private Access	The current Secure Private Access configuration lacks adaptive access policies, allowing potentially insecure access to applications. To enhance security, implement adaptive access policies that dynamically control access to enterprise web, SaaS, TCP, and UDP apps based on context. For granular controls, enable restricted access to enterprise web and SaaS apps by adding the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				security restrictions: **Clipboard**, **Screen capture**, **Printing**, **Key logging protection**, **Downloads**, **Uploads**, **Watermark**, and **Open in remote browser**.
Upgrade operating systems that reached End of Life	REC_024	High	VDA	Some machines are running operating systems (OS) that have reached End of Life. This poses significant security risks and may result in loss of support from both Citrix and the OS vendor. To maintain a secure and stable environment, ensure all your VDAs run a supported operating system.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
Upgrade hypervisor versions that reached End of Life	REC_025	Security	Hypervisor	Details: Some hypervisors are running versions that have reached End of Life. This poses a risk to environment stability and limits Citrix's ability to provide full support. To maintain a secure, supportable environment, upgrade to a vendor-supported hypervisor version. Regularly review vendor release notes and compatibility documentation to stay aligned with leading practices and platform requirements.
Use HTTPS for host connections	REC_039	Medium	General	Some host connections are currently configured with HTTP instead

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				of HTTPS. To ensure secure communication with your hypervisor, update these connections to use HTTPS. This requires enabling HTTPS on your hypervisor and ensuring valid TLS certificates are in place.
Address VDA security vulnerabilities	REC_040	High	VDA	Security vulnerabilities impact some of your VDA versions. Review the Citrix Security Bulletin and apply the necessary fixes or mitigations to ensure system integrity and compliance.
Address Citrix Workspace app security vulnerabilities	REC_041	High	Workspace app	Security vulnerabilities impact some Citrix Workspace app versions on endpoint devices. Review the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				Citrix Security Bulletin and apply the necessary fixes or mitigations to ensure system integrity and compliance.
Upgrade StoreFront server versions that reached End of Life	REC_043	High	StoreFront	Some StoreFront servers are running versions that have reached End of Life and are no longer supported by Citrix. To maintain a secure, supportable environment, upgrade all affected StoreFront servers to the latest LTSR or CR version.
Use HTTPS for StoreFront base URL	REC_044	High	StoreFront	Some StoreFront base URLs are currently configured with HTTP instead of HTTPS. To protect user credentials and sensitive data,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				configure your StoreFront servers and associated load balancers to use HTTPS. Make sure the base URL begins with 'https://'. This ensures all communications are encrypted and helps prevent security threats such as man-in-the-middle attacks.
Use HTTPS for communication between StoreFront and Cloud Connectors	REC_045	High	StoreFront	Traffic between StoreFront and Cloud Connectors is currently transmitted over unencrypted HTTP, which can expose user credentials to security threats. To protect your environment, enable HTTPS on Cloud Connectors and configure StoreFront to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				use secure connections.
Review StoreFront stores with anonymous access enabled	REC_052	Medium	StoreFront	Anonymous access is enabled for some StoreFront stores, allowing users to launch applications without authentication. To mitigate potential security risks, review these stores and remove unused ones.

NOTE:

StoreFront-related recommendations require additional setup. See Set up StoreFront for Advisor check for details.

Reliability recommendations

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
Configure restart schedules for multi-session delivery groups	REC_004	High	VDA	Some multi-session delivery groups do not have restart schedules configured. Scheduled restarts help

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				maintain optimal performance, stability, and resource availability across multi-session OS VDAs. To ensure service continuity and reduce downtime, create at least two restart schedules. Alternate restart schedules with tag restrictions by tagging VDAs into groups, such as 'Even' and 'Odd.'
Alternate restart schedules for multi-session delivery groups	REC_005	Medium	VDA	Some multi-session delivery groups only have one restart schedule configured. To ensure service continuity and reduce downtime, create at least two restart schedules. Alternate restart schedules with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				tag restrictions by tagging VDAs into groups, such as 'Even' and 'Odd.'
Host applications on multiple VDAs	REC_006	High	VDA	Some published applications are hosted on only a single VDA, which can impact service continuity and lead to downtime risks. Ensure that each application is hosted on multiple VDAs in a delivery group to help maintain availability and reliability.
Enable service continuity for Citrix Workspace	REC_007	High	Citrix Workspace	Service continuity isn’t enabled, which means that during a service disruption, users might not be able to launch sessions. Enable service continuity to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				improve availability by adding an extra layer of resiliency that maintains end-user access to apps and desktops despite network or service health.
Upgrade VDAs to match the catalog functional level	REC_008	High	VDA	Some machines use an earlier VDA version not supported by the minimum catalog functional level, which can prevent them from registering. To avoid registration issues, upgrade earlier VDA versions to match the catalog functional level.
Deploy Cloud Connectors in your zones	REC_014	High	Cloud Connector	Fewer than two Cloud Connectors are deployed in some of your zones

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				(resource locations). Deploy at least two Cloud Connectors per resource location to maintain availability and resiliency during Connector updates. Resource locations should follow the N + 1 model, where N is the baseline requirement based on deployment size and the additional 1 provides redundancy.
Schedule Connector updates	REC_015	Medium	Cloud Connector	Some zones (resource locations) don't have a scheduled start time for Connector updates. To ensure that updates only occur during planned maintenance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				windows and reduce service disruption, schedule Connector updates for a preferred time and day of the week.
Place Cloud Connectors in the same domain	REC_028	Medium	Cloud Connector	Some zones (resource locations) contain Cloud Connectors joined to different domains. This setup can lead to delayed or failed VDA registrations, especially when in Local Host Cache (LHC) mode. To improve reliability and reduce risk, ensure all Cloud Connectors within a given zone belong to the same domain.
Enable communication between	REC_029	High	Cloud Connector	Some zones (resource locations) have

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
Cloud Connectors for reliable LHC performance				multiple elected Local Host Cache (LHC) brokers. This can cause VDA registrations to be divided among the Cloud Connectors in LHC mode, leading to intermittent launch failures. To prevent this, ensure all Cloud Connectors in each affected zone can communicate with one another at http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection.
Check resiliency configurations	REC_030	Medium	General	Your deployment resiliency configurations have not been verified recently. Maintaining proper

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				resiliency configurations is critical for ensuring uninterrupted access to apps and desktops, especially during unexpected service disruptions. Check your resiliency configurations regularly to ensure your deployment is properly set up to handle potential disruptions and safeguard user productivity.
Enable advanced health check for StoreFront stores	REC_036	Medium	StoreFront	One or more stores on some StoreFront servers do not have advanced health check enabled. StoreFront uses the additional information from the advanced health check results to ensure launch

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				requests are sent to the appropriate resource location (zone) in Local Host Cache (LHC) mode. Without advanced health check, launches may fail when in LHC mode. To improve the resiliency of your Citrix environment, enable advanced health check for all stores on the StoreFront servers.
Add all Cloud Connectors as STA servers on StoreFront and NetScaler Gateway	REC_037	Medium	Cloud Connector	Some Cloud Connectors are not configured as Secure Ticket Authority (STA) servers, which is preventing them from receiving STA requests from StoreFront. To avoid launch failures in Local Host Cache mode, ensure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				all Cloud Connectors are added as STA servers on both StoreFront and NetScaler Gateway.
Ensure StoreFront server redundancy	REC_042	High	StoreFront	Some StoreFront server groups contain only one server, creating a single point of failure and a lack of redundancy in the event of an outage. For better resiliency, deploy at least two StoreFront servers in a server group and front them with a load balancer to ensure seamless failover and uninterrupted access.
Check Cloud Connector communication with StoreFront	REC_047	Medium	StoreFront	Some resource locations (zones) contain Cloud Connectors that

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				are not receiving StoreFront requests for resource enumeration. This issue can occur if the Cloud Connectors are not listed in StoreFront or if there is a communication problem, such as an expired certificate on the Cloud Connector. Ensure that all Cloud Connectors are listed in StoreFront and are reachable. If you are not using an on-premises StoreFront deployment, ignore this recommendation.

NOTE:

StoreFront-related recommendations require additional setup. See Set up StoreFront for Advisor check for details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Performance recommendations

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
Optimize Cloud Connectors for LHC mode	REC_019	High	Cloud Connector	Some Cloud Connectors have less than four CPU cores per socket, which can impact users' ability to enumerate and launch available resources while in LHC mode. To maximize resource availability for LHC and prevent performance bottlenecks, configure Cloud Connector machines to have at least four cores per socket.
Enhance Cloud Connector hardware	REC_020	High	Cloud Connector	High CPU, memory, or disk usage might impact Cloud Connector performance and availability. To prevent performance degradation and maintain

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				reliability, increase CPU, memory, or storage for the Cloud Connectors.
Rightsize high resource-consuming machines	REC_023	Medium	VDA	Some machines show signs of performance strain, such as high CPU or memory utilization, or a high session count. This indicates machines are undersized to handle the workloads they support, which can lead to a poor user experience and reduced performance. Consider changing the machine size to increase the allocated resources for the machine or relocating power users to a delivery group that has high-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				performance machines.
Reduce the number of host connections in your zones	REC_026	High	General	The number of host connections in some zones (resource locations) exceeds the recommended limit, which might result in performance degradation. Reduce the number of host connections in the zones to no more than the recommended limit.
Reduce the number of VDAs in your zones	REC_027	High	VDA	The number of VDAs in some zones (resource location) exceeds the recommended limit, increasing the risk of failed VDA registrations and degraded session brokering, especially when in Local Host Cache (LHC)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				mode. To mitigate these risks, redistribute VDAs by moving some to other zones. Ensure your method for configuring VDA registration is updated accordingly.
Evaluate resource allocation for PVS servers	REC_031	Medium	Provisioning	Some Citrix Provisioning (PVS) servers show signs of performance strain, such as high CPU or memory utilization. Insufficient server resource allocation may result in poor performance and extended boot times. Consider increasing the CPU and memory allocation for these PVS servers as needed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
Increase resource allocation for PVS servers	REC_032	High	Provisioning	Some Citrix Provisioning (PVS) servers show signs of performance strain, such as critical CPU or memory utilization. Insufficient server resource allocation may result in poor performance and extended boot times. Consider increasing the CPU and memory allocation for these PVS servers as needed.
Evaluate write cache disk size for PVS target devices	REC_033	Medium	VDA	The write cache disk usage on some Citrix Provisioning (PVS) target devices is nearing the threshold. To avoid performance issues and user session failures, evaluate the current write

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				cache disk size and increase it as needed.
Optimize GPO configuration for VDAs	REC_035	Medium	VDA	Some user sessions experienced prolonged GPO processing during logon, impacting performance. To increase control over environment settings, block Group Policy inheritance for your VDA organizational units and apply only relevant policies and security configurations. Additionally, consider leveraging Citrix Workspace Environment Management to process settings asynchronously for faster session logons.
Enable socket pooling for	REC_046	Medium	StoreFront	Some StoreFront

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
StoreFront stores				stores don't have socket pooling enabled. Socket pooling enhances efficiency by maintaining a pool of readily available network connections (sockets) for communication with Delivery Controllers or Cloud Connectors. Instead of creating a new socket for every request and then closing it (a high-overhead process), StoreFront reuses an existing connection from the pool. To enhance overall environment performance and efficiency, enable socket pooling on all stores, particularly for Transport Layer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				Security (TLS) connections.
Place StoreFront servers in a low-latency network	REC_051	Medium	StoreFront	High latency was detected between servers in some server groups, which may lead to performance issues. Latency between servers in a group should be under 40 ms (with subscriptions disabled) or 3 ms (with subscriptions enabled). Place the servers in a low-latency network or separate them into different server groups.

NOTE:

StoreFront-related recommendations require additional setup. See Set up StoreFront for Advisor check for details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Operational excellence recommendations

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
Upgrade VDAs to the latest version	REC_002	Low	VDA	Some machines are using older VDA versions. Upgrade to the latest LTSR or CR VDA version to access new features, improvements, and security enhancements.
Use Citrix provisioning technology	REC_003	Medium	Provisioning	All machines in the site are manually provisioned and do not use Citrix provisioning technologies such as Machine Creation Services (MCS) or Citrix Provisioning Services (PVS). Use MCS or PVS to ensure VDA consistency, minimize manual tasks, and streamline environment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				scaling operations.
Low functional level	REC_009	Low	VDA	Some machine catalogs have a lower functional level than the detected VDA version, limiting access to new features on later VDA versions. To access these features, change the functional level to the latest version supported by all machines in the catalog.
Back up your site configuration	REC_011	High	General	You don't have a backup of your site configuration. Create on-demand or scheduled backups to ensure you have a ready-to-use copy of your Citrix configurations for quick recovery.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
Create a new backup of your site configuration	REC_012	High	General	Your last site configuration backup was over three months ago. Regularly create on-demand or scheduled backups to keep an up-to-date copy of your Citrix configurations ready for quick recovery.
Simplify catalog configuration with a machine profile	REC_038	Low	Provisioning	Some machine catalogs would benefit from using a machine profile. With a machine profile, Machine Creation Services (MCS) captures hardware properties and hypervisor-specific features from the profile and efficiently provisions new virtual machines (VMs) in the catalog with the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				same configuration.
Reset tainted Active Directory accounts	REC_049	Medium	Provisioning	Some machine catalogs contain AD accounts marked as 'tainted' in the AD Identity Service. These accounts must be reset to be available for subsequent provisioning operations.
Replace deprecated beacon point for StoreFront	REC_050	Medium	StoreFront	Citrix Workspace app uses beacon points configured within StoreFront to determine whether users are connected to internal or external networks. You are using ping.citrix.com as a beacon, which has been deprecated and is no longer reachable. Replace it with a reachable,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				public-facing URL in the StoreFront management console.
Disable XenApp Services URL for StoreFront stores	REC_053	High	StoreFront	The XenApp Services URL (also known as PNAgent) is enabled for some StoreFront stores. This feature is deprecated. For compatibility and security, configure Citrix Workspace app to connect to StoreFront using the Store URL, and disable XenApp Services on the server. If you have legacy devices that require PNAgent, ignore this recommendation.
Deprecate unsupported StoreFront sites	REC_054	High	StoreFront	Some StoreFront stores are linked to unsupported

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				site types. Migrate resources to supported sites and deprecate the unsupported sites.
Disable Kerberos delegation for StoreFront stores	REC_055	Low	StoreFront	Kerberos delegation is enabled for some StoreFront stores. Kerberos delegation is deprecated and can only be used with XenApp 6.5 and earlier. Disable Kerberos delegation for these StoreFront stores.
Review machines in maintenance mode for extended periods	REC_056	Medium	VDA	Some machines have been in maintenance mode for over 14 days. Review the machines to determine if they should be returned to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
				service, decommissioned, or kept in maintenance mode with justification.
Reduce troubleshooting time with Always On Tracing	REC_058	Medium	General	Add a log server to securely transfer your Always On Tracing (AOT) logs to a centralized log server. Logs are collected in real time and available in Monitor, helping you resolve problems faster and streamline support investigations.

NOTE:

StoreFront-related recommendations require additional setup. See Set up StoreFront for Advisor check for details.

Cost optimization recommendations

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
Enable Autoscale for	REC_010	Medium	VDA	Some eligible delivery groups aren't using

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION	ID	IMPACT	COMPONENT	DESCRIPTION
your delivery groups				Autoscale. Enable Autoscale for consistent machine power management, maintaining availability while effectively balancing costs and user experience.
Release unused resources	REC_013	Medium	General	Some dedicated workloads, such as machines or applications, have not been used for over 30 days. To reduce unnecessary spending and optimize costs, release unused machines back to the available pool and manage unused applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA Upgrade Service (VUS)

The Citrix VDA Upgrade Service (VUS) is a component of Citrix Desktop as a Service (DaaS) that facilitates a streamlined upgrade process for persistent Virtual Delivery Agents (VDAs) within your Citrix environment. The service helps keep your environments up to date with the latest VDA versions, enhancing performance and security, and enabling new Citrix DaaS™ features.

NOTE:

Before scheduling an upgrade, the VDA Upgrade Service checks that each VDA's current operating system is supported by the selected target version. If a VDA runs an operating system that the target version no longer supports, that target is not offered for the VDA, and the VDA is reported as Up to date.

Administrators can leverage VUS to check for updates, schedule upgrades, and monitor upgrade progress. Upgrades can be initiated immediately or scheduled for a specific date and time, enabling you to choose the best time for your upgrades.

Upgrading VDAs has never been easier. Install the VDA Upgrade Agent on your VDAs or images, right-click on the machine or machine catalog in the full configuration interface, select “Upgrade VDAs,” and select the options that best fit your environment.

Before upgrading, review the upgrade cycle options. Two upgrade tracks are available for your VDAs: Long-Term Service Release (LTSR) and Current Release (CR). LTSR has a longer support lifecycle, providing more stability and less frequent upgrades. CR versions are released more frequently, providing the latest and greatest features. For more information, refer to Lifecycle Milestones.

Prerequisites for upgrading VDAs using VUS

To perform VDA upgrades using VUS, the following prerequisites must be met.

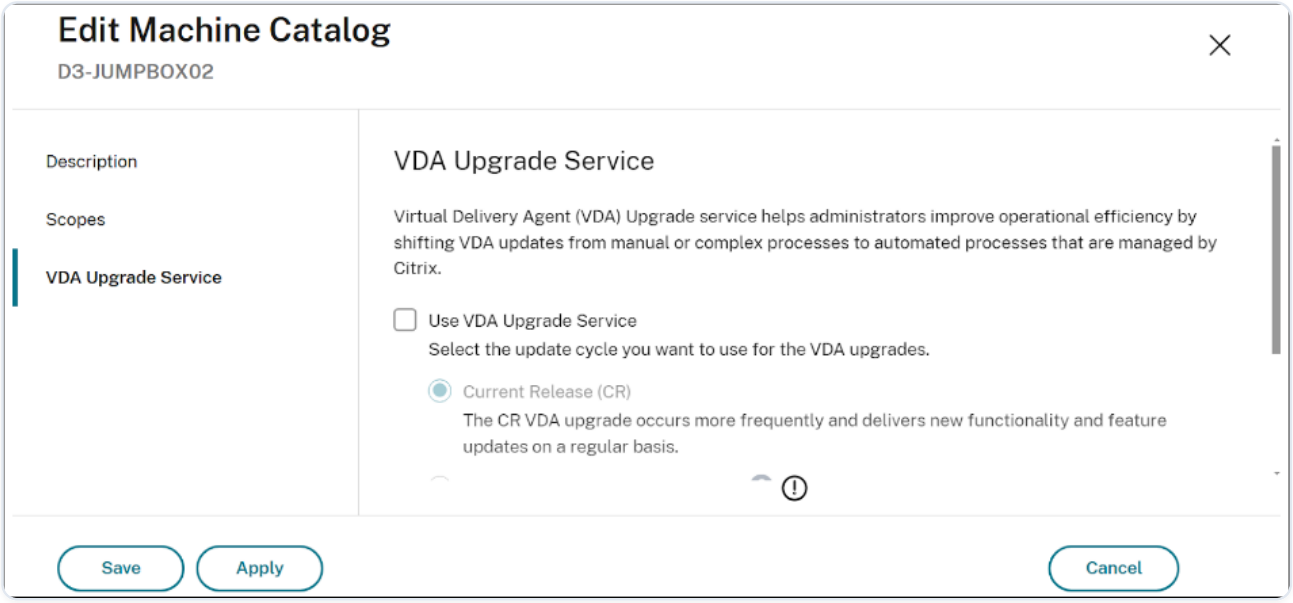
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable the VDA Upgrade Service

To enable the VDA Upgrade Service feature, use the VDA Upgrade option when creating or editing a Machine Catalog. Admins must choose from the following upgrade cycles when enabling the VUS:

- LTSR
- CR
- LTSR Early Access Release (EAR)
- CR EAR

To enable the VDA Upgrade Service for a machine catalog from the DaaS full configuration interface, right-click on a catalog, click “Edit Catalog”, select the “VDA Upgrade Service” tab, check the “Use VDA Upgrade Service” box, and select an upgrade track.



To enable the VDA Upgrade Service for a machine catalog using PowerShell, use the `Set-VusCatalogUpgradeType` cmdlet.

The upgrade type can be set as “LTSR”, “CR”, “EAR_CR”, or “EAR_LTSR”.

Example: `Set-VusCatalogUpgradeType -CatalogName "Workstation catalog" -UpgradeType LTSR`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Enabling the VDA Upgrade option will not result in the automatic upgrade of VDAs. All VDA upgrades through VUS must be initiated as a separate task explicitly performed by administrators.

VDA Requirements

VDA Version

2109 CR or later, or 2203 LTSR or later

Source VDA operating system

The VDA Upgrade Service only offers a target version whose system requirements include the VDA's current operating system. If a VDA runs an operating system that has been removed from support in the target version - for example, Windows Server 2016, which is not supported as a VDA OS from CVAD 2407 onward - that target is not offered, and the VDA is reported as Up to date with no available upgrade. To upgrade such a VDA, re-image it to a supported operating system. For the operating systems each version supports, see the System requirements for that version and CTX224843.

Provisioning Type

- Single or multi-session persistent machines provisioned using non-Citrix provisioning™ services or technologies.
- Single-session MCS-provisioned persistent machines (AD joined, Microsoft Entra joined, and non-domain-joined).
- Remote PC Access machines.
- Citrix HDX™ Plus for Windows 365.

VDA Upgrade Agent

- The VDA Upgrade Agent must be installed and active on the VDA. The agent can be installed:
    - As an additional component, when upgrading your VDA or modifying the VDA installation.
    - Using the standalone MSI that is available in the Citrix Virtual Apps and Desktops™ iso.
        - MSI name: CitrixUpgradeAgent_x64.msi
        - Path: x64\Virtual Desktop Components

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To upgrade LTSR VDAs to LTSR CU versions, the VDA Upgrade Agent must be version 7.36.0.7 or later.

  NOTE:

  The VDA upgrade agent updates automatically if the VDA has access to the URLs listed in Connectivity.

Permissions

You must have the Full Administrator or Machine Catalog Administrator role in Citrix DaaS.

VDA State

For upgrades scheduled through VUS to proceed as intended, the VDAs targeted for upgrade must meet the following prerequisites:

- The VDA must not be manually put in maintenance mode.
- For a VDA upgrade to occur successfully, no users can be logged on.
  - VDAs are placed in maintenance mode when the upgrade process begins draining user sessions throughout the upgrade window. They are removed from maintenance mode once the upgrade is completed successfully.
  - If a user has an active or disconnected session throughout the duration of the upgrade window, the upgrade will be canceled at the end of the Upgrade Window.

    NOTE:

    Active and disconnected sessions can be terminated using the forced logoff option in VUS.

  - VDAs not provisioned through MCS (manually provisioned) must be added to a Delivery Group before performing an upgrade through VUS.
  - VDAs must be powered on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> AutoScale™ does not cease power managing machines when VDA upgrades are scheduled. Consider disabling AutoScale schedules on the Delivery Group when upgrades are in progress.

Connectivity

- VDAs must be able to communicate with the following URLs:
  - If using the Citrix content delivery network (CDN) for downloading the VDA installer, VDAs must be able to communicate with the following URLs.
    - Production - Gov: `<https://prod-us-gov-vus-release-endpoint-*.z01.azurefd.us/prod-us-gov-vus-release-container/*>`
    - Production - United States (US): `<https://prod-us-vus-storage-endpoint.azureedge.net/*>`
    - Production - European Union (EU): `<https://prod-eu-vus-storage-endpoint.azureedge.net/*>`
    - Production - Asia Pacific South (APS): `<https://prod-aps-vus-storage-endpoint.azureedge.net/*>`
    - Production - Japan (JP): `<https://prod-jp-vus-storage-endpoint.azureedge.net/*>`
  - To verify that the VDA installer is signed by a valid certificate, VDAs must communicate with the following URLs. Applicable to Production Gov as well no change.
    - http://crl3.digicert.com/*
    - http://crl4.digicert.com/*
    - http://ocsp.digicert.com/*
    - http://cacerts.digicert.com/*
  - The VDA Upgrade Agent communicates with DaaS at the following URLs.
    - Production Gov https://.xendesktop.us/citrix/vdaupdateservice/*
    - https://.xendesktop.net/citrix/VdaUpdateService/*, where is the customer ID parameter displayed on the Secure Clients tab (Identity and Access Management > API Access > Secure Clients) of the Citrix Cloud management console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDAs with Proxy configurations

- Supported for VDA Upgrade Agent version 7.40 and higher.
- Only proxies in the form of Hostname: Port (IP:Port) and PAC file are supported. SOCKS5 proxies are not supported.
- The VDA Upgrade Agent must be configured to use a proxy using the full configuration interface or the registry.
    - VDA Upgrade Agent proxy configuration using the full configuration interface
        - Enable the VDA upgrade proxy configuration Citrix Policy setting for the VDAs that use a proxy.
        - Input the proxy address or the path to the PAC file in the settings.
    - VDA Upgrade Agent proxy configuration using the registry
        - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
            - Value type: String
            - Value name: ProxySettings
            - Value data: Proxy address or path to pac file.
            - For example:
                - Proxy address: http://<URL or IP>:\<port>
                - Pac file: http://<URL or IP>/\<path/\<filename>.pac
- Certificate validation uses the Windows CryptoAPI, which does not support proxy communication.
    - To configure the system proxy on the VDA to facilitate outbound CRL calls. Input one of the following commands into the command line of the VDA to configure the system proxy:
        - To copy proxy settings from Internet Explorer:
            - netsh winhttp import proxy source=ie
        - To utilize a separate proxy setting:
            - netsh winhttp set proxy proxy-server=http://Proxy_Server:Port

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDAs installed using the VDAWorkstationCoreSetup.exe

If the VDA was originally installed using `VDAWorkstationCoreSetup.exe`, it can still be upgraded using VUS, which utilizes VDAWorkstationSetup.exe. When upgrading VDAs that were installed with `VDAWorkstationCoreSetup.exe` using VUS, you should review the installation options to ensure only the desired features are enabled, especially if migrating from a minimal core installation.

Government Cloud prerequisites for VDA upgrades (VUS)

This article documents customer-side prerequisites for upgrading VDAs through the VDA Upgrade Service (VUS) in the Production Government environment.

Use this guidance when outbound firewall or proxy controls are enforced and egress is restricted.

Pre-requisites

These prerequisites apply to Government customers who use VUS to upgrade persistent VDAs and need to allow required outbound connections for package download, schedule retrieval, and version reporting.

This guidance is in addition to the standard VUS prerequisites in Prerequisites for upgrading VDAs using VUS.

Required outbound endpoint access

Allow outbound HTTPS (TCP 443) from the following sources:

- VDAs that run the VDA Upgrade Agent.
- Cloud Connectors, when traffic is connector-routed.

Allow-list the following destination patterns:

- Prod Government VUS release CDN endpoint pattern: https://prod-us-gov-vus-release-endpoint-*.z01.azurefd.us/prod-us-gov-vus-release-container/*
- Per-customer Government DDC REST endpoint pattern: https://.xendesktop.us/citrix/vdaupdateservice/*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Why these endpoints are required

ENDPOINT PATTERN	PURPOSE	USED BY
https://prod-us-gov-vus-release-endpoint-*.z01.azurefd.us/prod-us-gov-vus-release-container/*	Downloads VDA installer packages for scheduled upgrades.	VDA Upgrade Agent download flow
https://[customerId].xendesktop.us/citrix/vdaupdateservice/*	Gets VUS schedules and posts VDA version report calls.	VDA Upgrade Agent control plane calls

If either endpoint is blocked by firewall, proxy, SSL inspection policy, or DNS filtering, upgrades can fail.

Government storage and KeyVault pre-requisites

Government storage account and KeyVault resources used by the VUS release pipeline are managed on the service side.

Customer action is typically limited to network egress policy configuration for VDAs and Cloud Connectors. If your organization applies additional outbound controls or private routing constraints, coordinate validation with your Citrix support and security teams before scheduling production upgrades.

FedRAMP boundary considerations

- Review your FedRAMP boundary controls for outbound HTTPS to Azure Government Front Door endpoints (*.azurefd.us) and customer-specific xendesktop.us endpoints.
- Document approved destination patterns and control rationale in your SSP and change records.
- If TLS inspection is mandatory, validate that certificate handling does not break VDA installer download or API communication.

Pre-upgrade verification checklist

- Confirm DNS resolution and TCP 443 reachability from each VDA subnet to the required *.azurefd.us endpoint.
- Confirm DNS resolution and TCP 443 reachability from each VDA subnet to https://.xendesktop.us.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Confirm the same reachability from Cloud Connectors for connector-routed traffic paths.
- Run a pilot VUS upgrade on a small machine set and verify package download and version report success.

Upgrade VDAs using VUS

You can initiate VDA upgrades through the VDA upgrade service by selecting the target machine catalog, individual machine, or group of machines and then selecting “Upgrade VDAs”.

NOTE:

Citrix® recommends backing up VDAs before performing upgrades when possible.

Scheduling Upgrades

The VDA upgrade process in Citrix can be carried out on a catalog level, a group of machines level, or an individual machine level, depending on the requirements. Upgrades can be set to start immediately or can be scheduled at a date and time up to 7 days in advance.

Considerations

- **Catalog vs. Group of Machine vs. Machine Scope:** Catalog upgrades are ideal for bulk updates while upgrading machines individually or by groups allows more granular control.
- **Scheduling:** Upgrades can be scheduled for up to 7 days in advance. If using machine catalog level upgrades, machines added to the catalog after the upgrade is scheduled are not included as part of the existing scheduled upgrade.

Restrict upgrades to tagged machines

At the machine catalog level, you can now limit VDA upgrades to only machines that carry a selected machine tag.

In Web Studio, when you initiate a catalog-level upgrade, choose **Upgrade machines that match the tag** instead of **Upgrade all machines**. Then select a tag from the tag picker.

Only machines in that catalog with the selected tag are included in the upgrade scope.

This option supports both CR and LTSR upgrade tracks.

Use this option for ring-based rollout strategies when you want to validate a newer VDA version on a pilot subset before scheduling upgrades for the full catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scope

- Available for catalog-level upgrades only.
- Not available for delivery group-level upgrades.
- Not available for individual machine-level upgrades.

UI behavior

When you select **Upgrade machines that match the tag**:

- A tag picker appears and shows tags present in the selected catalog.
- The machine count on the **Schedule** page reflects only tagged machines in scope.
- The machine count on the **Summary** page reflects only tagged machines in scope.

Key Differences

FEATURE	PER-CATALOG UPGRADE	PER-MACHINE UPGRADE	GROUP OF MACHINES
Scope of upgrades	Entire catalog	Individual machine	Group of machines from a Machine Catalog
Schedule control	A single schedule applies to all VDAs in the machine catalog, best for large-scale upgrade operations	VDAs are scheduled individually, which is mostly used for testing and one-off upgrades	VDAs are scheduled in groups, giving you the flexibility to upgrade different groups of VDAs at different times
Management	Managed through machine catalogs node in the Full Configuration interface or the `New-VusCatalogSchedule` cmdlet	Managed through Search node in the Full Configuration interface or the `New-VusMachineUpgrade` cmdlet	Managed through the Search node in the Full Configuration interface, or by passing a list of machines to the `New-VusMachineUpgrade` cmdlet

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	PER-CATALOG UPGRADE	PER-MACHINE UPGRADE	GROUP OF MACHINES
Use Case	Bulk upgrades for an entire Machine Catalog	Granular control for targeted upgrades and test scenarios	Targeted control of a subset of VDAs. Can be used to stagger the upgrades within a catalog
VDA versions available	For CR and all currently supported LTSR VDA versions, the latest version as well as 2 previous (N-2) versions are available to upgrade to. See VDA versions available for more information	For CR and all currently supported LTSR VDA versions, the latest version as well as 2 previous (N-2) versions are available to upgrade to. See VDA versions available for more information	Only the latest LTSR or CR VDA version is available to be upgraded
Additional Components	Installs or upgrades VDA components on each VDA. Leaving a component unchecked will not uninstall the feature, but the component will not be upgraded	Installs or upgrades the VDA component on the VDA. Leaving a component unchecked will not uninstall the feature, but the component will not be upgraded	Additional components cannot be managed by the VDA upgrade service when upgrading a group of machines. Note: Additional features, like “Enable Restore Cleanup” is available for group of machine upgrades
Additional Features	Additional features can be enabled or upgraded	Additional features can be enabled or upgraded	Additional features can be enabled or upgraded
Concurrency	Controlled as a setting when scheduling the upgrade. See Concurrency for more information	A single VDA is upgraded	Automatically load balanced based on the number of VDAs selected as part of the upgrade schedule

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	PER-CATALOG UPGRADE	PER-MACHINE UPGRADE	GROUP OF MACHINES
Failure Threshold	A failure threshold can be set to prevent future upgrades if a provided number of VDAs fail upgrades. See Failure Threshold for more information	Failure thresholds are not applicable for a per-machine upgrade	Failure thresholds are not available for group of machine upgrades. Consider setting the size of the group of machines to be upgraded to be the maximum number of VDAs that would be an acceptable failure amount

How scheduled upgrades work

The VDA Upgrade Agent on the VDAs communicates with Citrix Cloud™ periodically to determine if the VDA should be upgraded. VDAs can be scheduled to upgrade immediately or up to 7 days in advance. When scheduling an upgrade in advance, you can set the date and time (in UTC) that the upgrade begins.

The upgrade duration sets the length of time after the scheduled upgrade start time during which upgrades occur. By default, for machine catalog and group of machine upgrades, Citrix load balances VDA upgrades throughout the upgrade duration to improve performance and avoid bottlenecks.

Once an upgrade begins, the VDA is placed into maintenance mode until the upgrade is complete. If a session is present on the VDA, the VDA will not upgrade until no sessions are present. No new sessions can be brokered to the VDA when it is in maintenance mode. If a user disconnects from a session during an upgrade window, the user will not be able to reconnect until the upgrade is complete.

The VDA will continue to attempt an upgrade until the scheduled upgrade duration is complete. If a session is present throughout the upgrade duration, the upgrade will be canceled, and maintenance mode will be turned off for the VDA. Consider a longer upgrade duration to improve the VDA upgrade success rate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

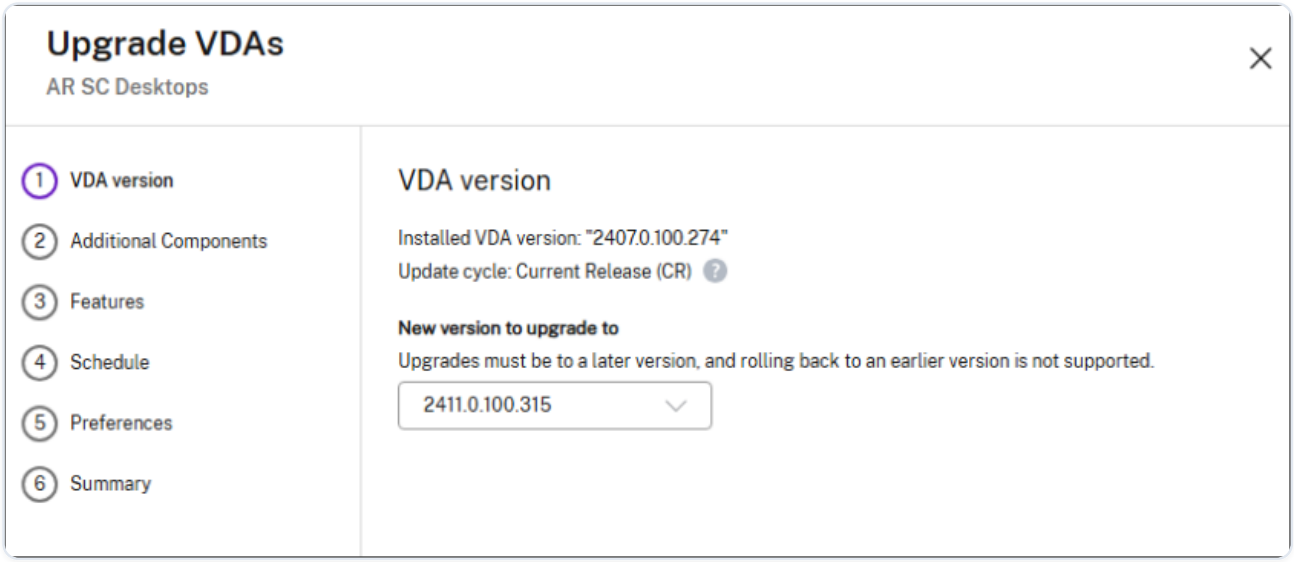
VDAs manually placed into maintenance mode before a scheduled upgrade will fail to upgrade.

VDA Versions Available

New VDA versions are available to upgrade through the VDA upgrade service shortly after the new VDA versions are made generally available. The VDA upgrade service maintains N-2 versions of the VDA for CR versions and N-2 CU versions for all LTSR versions that are currently supported.

The Upgrade VDAs wizard lists only the target versions compatible with each selected VDA's current operating system. A target that has removed support for a VDA's operating system is not shown for that VDA.

In the full configuration interface, when upgrading either a catalog or an individual machine, the UI prompts you for which version you want to upgrade your VDAs to.



To determine the available VDA versions using PowerShell, use the `Get-VusAvailableVdaVersion` cmdlet.

Without passing a machine or a catalog with the cmdlet, the cmdlet will return the latest available version for all upgrade tracks.

To get the specific versions available for a resource, pass a VDA (-MachineName, -MachineUid or -MachineUuid) or catalog (-CatalogName, -CatalogUid, or -CatalogUuid) with the `Get-VusAvailableVdaVersion` cmdlet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

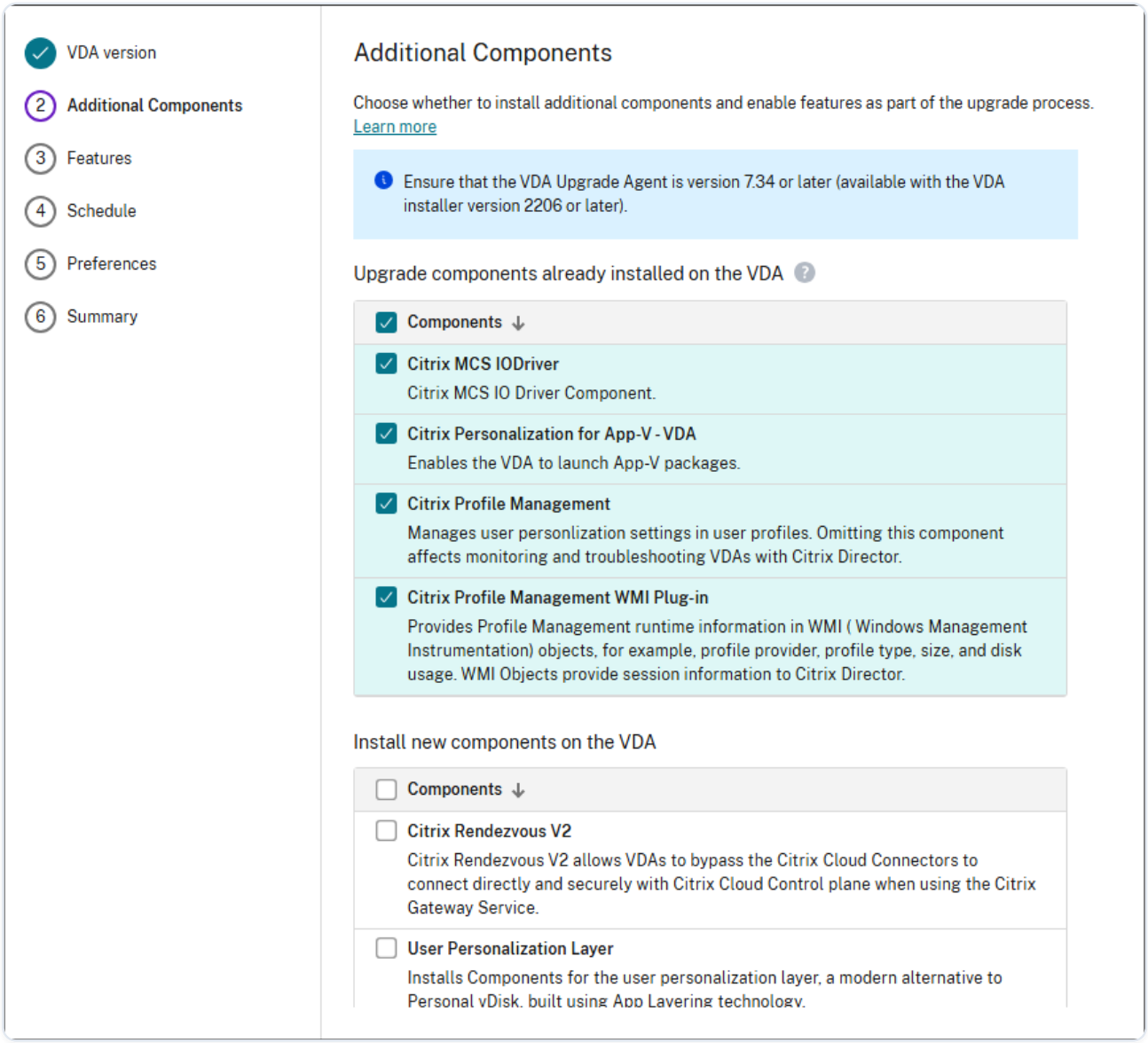
For example: `Get-VusAvailableVdaVersion -CatalogName '[Name of your Machine Catalog]'`

```
PS V:\> Get-VusAvailableVdaVersion -CatalogName 'CR-2303'

UpgradeType Version
----------- -------
         CR 2411.0.100.315
         CR 2407.0.100.274
         CR 2402.0.100.629
```

Additional Components

Additional components can be installed or upgraded when upgrading VDAs by machine catalog or by individual machine. If you do not check a component, it will not uninstall the component, but the component will not be upgraded as part of the overall VDA upgrade.

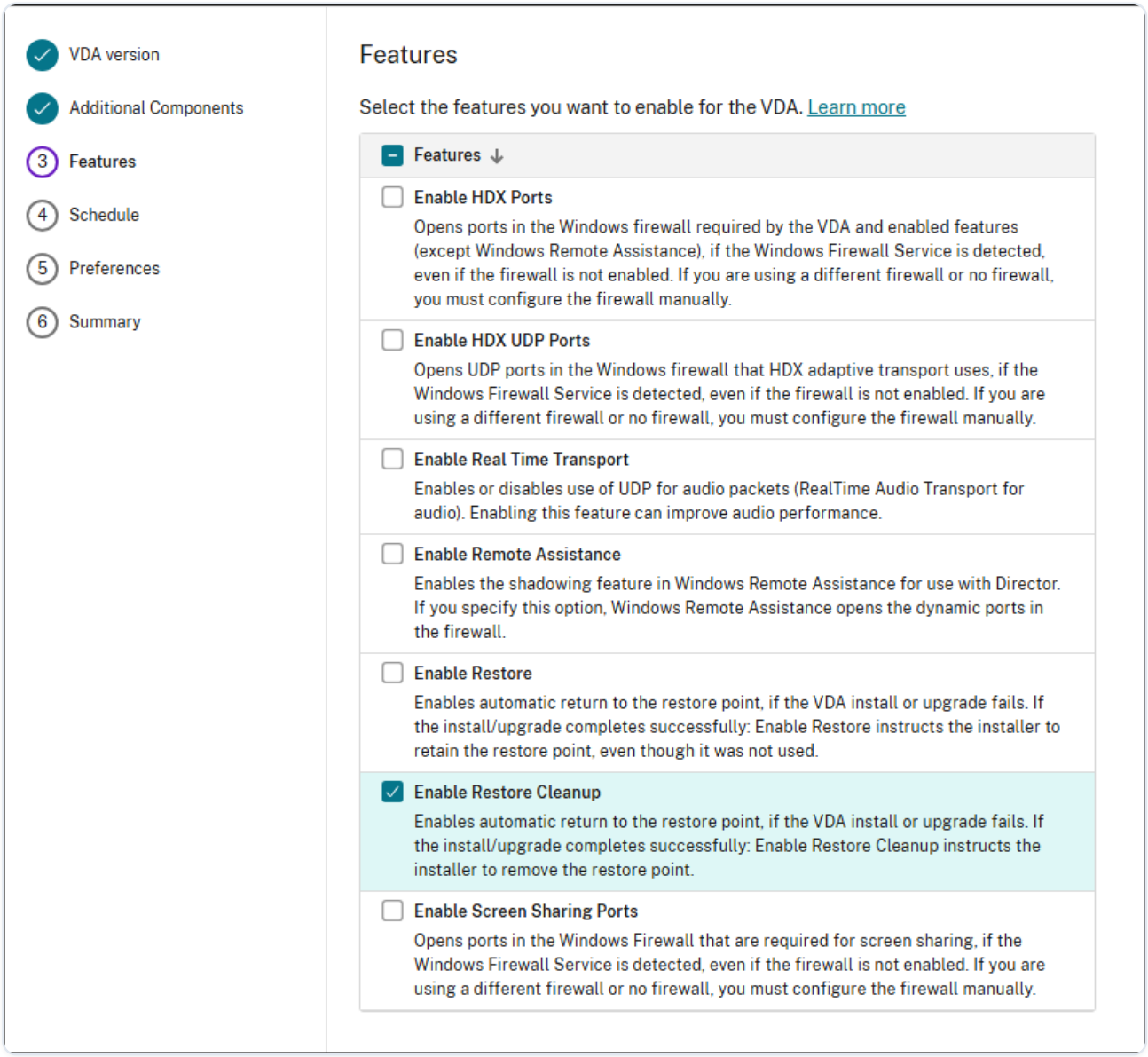


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Features

Features can be enabled or upgraded on VDAs through the VDA upgrade service. If you do not check a feature, it will not disable the feature, but the feature will not be upgraded as part of the overall VDA upgrade.

By default, the **Enable restore cleanup** checkbox is selected. Citrix recommends enabling the restore cleanup feature to ease management and improve recovery of failed upgrades. With the feature enabled, a system restore point is created before the upgrade starts. If an upgrade fails, the VDA is restored to the system restore point. The restore point is deleted after the successful installation of the VDA. For more information, see Restore on install or upgrade failure.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Windows System Restore is only supported on single-session operating systems (e.g., Windows 10 and 11). The Windows System Restore feature must be enabled on the VDA for the “Enable restore cleanup” feature to work. Upgrades may fail if “Enable restore” or “Enable restore cleanup” is selected, but Windows System Restore is not configured on the VDA.

Concurrency

When upgrading machine catalogs, VUS enables you to define a maximum number of VDAs that will upgrade simultaneously. This can help reduce the load on your internet connection or file server and, when used in conjunction with failure thresholds, enables you to stop upgrades if a number of VDAs fail to upgrade.

As soon as the scheduled upgrade starts, all VDAs in the catalog are placed in maintenance mode. An upgrade will start on a quantity of VDAs that matches the defined maximum concurrency setting. As soon as a VDA upgrade is completed, another VDA will begin to upgrade to maintain the concurrent number of VDAs upgrading simultaneously.

If no concurrency is specified for a machine catalog scheduled upgrade, Citrix uses a default concurrency value based on the total number of VDAs in the Catalog and the upgrade duration.

Upgrades take an average of around 30 minutes to complete, but this can vary greatly based on environmental conditions. Consider setting your concurrency to a quantity where all VDAs can upgrade in the provided upgrade duration. For example, if you have 20 VDAs that are set to upgrade over 4 hours, you need 5 VDAs to upgrade an hour. Using the average upgrade duration of 30 minutes, you can set the concurrency value to 3 to meet the 5 VDA upgrades per hour requirement (3 upgrades per 30 minutes results in 6 updates per hour).

Failure Threshold

When upgrading machine catalogs, use a failure threshold to prevent further VDAs from being upgraded if a given number of VDAs have failed. Failure thresholds can reduce the impact radius of issues that cause upgrade failures, reducing troubleshooting efforts for administrators.

Failure thresholds prevent any future VDAs from starting upgrades, but do not stop VDAs that have already started the upgrade. For example, if a machine catalog has 100 VDAs, concurrency is set to 10 VDAs, and the failure threshold is set to 3, if all VDA upgrades fail, at least 13 VDAs will have attempted to upgrade, and the remaining 87 will have never started, and the upgrade will be cancelled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10 concurrent VDAs start to upgrade at the beginning of the scheduled upgrade, if the first upgrade fails, another VDA will start the upgrade to maintain the 10 concurrent simultaneous upgrades. If the second upgrade fails, another VDA will begin the upgrade. If the third upgrade fails, all VDAs that are currently in the upgrade process will continue, and the rest of the VDAs in the upgrade schedule will have their upgrade cancelled.

VDA Installer Location

You can choose for VDAs to download the VDA installation media from either the Citrix-hosted CDN or a local file share.

Upgrades through a locally hosted file share reduce the requirement for providing network rules to allow VDAs to fetch the installation media and can decrease bandwidth utilization during the upgrade process.

If using the Citrix-hosted CDN, VDAs must be able to communicate with the URLs listed in Connectivity.

If using a local file share, the file share must have the following prerequisites.

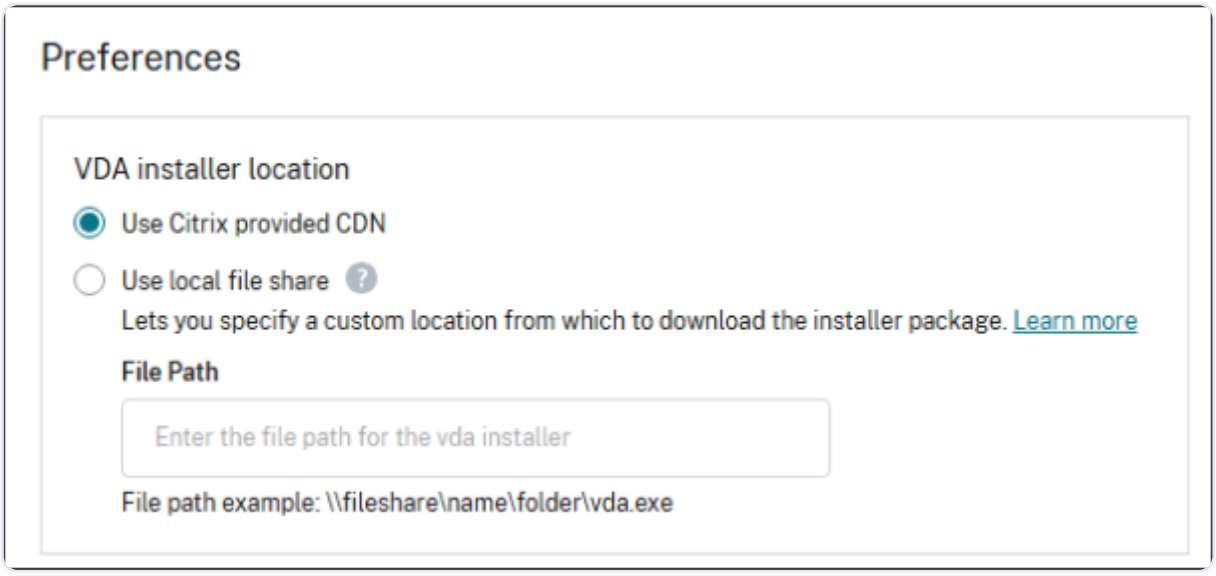
- The VDA Upgrade Agent must be version 7.40.0.35 or later, which is installed by default on VDA version 2311 or later.
    - The VDA Upgrade Agent does not require a scheduled VDA upgrade to upgrade. The VDA Upgrade Agent updates automatically.
- If upgrading using PowerShell, the Virtual Apps and Desktops Remote PowerShell SDK version 7.42 or newer must be installed.
- File Share Permissions
    - The network shares containing VDA installer packages must have read access for the VDA Upgrade Agent service which runs as Local System (NT AUTHORITY\SYSTEM principal).
    - Domain-Joined VDAs:
        - The Local System account (VUA runs as Local System), uses computer credentials when accessing network shares.
        - The file share must be given read access to Domain Computers.
        - In Advanced Share Settings, **File and Printer Sharing** must be enabled.
    - Non Domain-Joined VDAs:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - The Local System account (VUA runs as Local System), uses **ANONYMOUS LOGON** when accessing network shares.
    - In the **Network and Sharing Center, Password Protected Sharing** must be disabled.
    - In the folder permissions **Security** tab, read access permissions must be granted to **ANONYMOUS LOGON**.
    - In Advanced Share Settings, **File and Printer Sharing** must be enabled.
    - The shared folder name must be added to the **Network Access Security Policy**.

- VDA installer
    - The VDA installer must be downloaded from the Citrix Downloads website and placed in the file share.
    - The relevant VDA installer for the machine catalog must be downloaded.
        - Use the **Multi-session OS VDA installer** if the catalog type is multi-session.
        - Use the **Single-session OS VDA installer** if the catalog type is single-session.
    - For a given upgrade, the version of the installer on the file share must be an excat match of a version published by VUS. Use the `Get-VusAvailableVersion` PowerShell cmdlet to determine the available versions.

To set VDAs to upgrade from a local file share in the Full Configuration interface, select “Use local file share” in the VDA installer location and input the path to the installer. For example, `"\\hostname\VDA-Packages\VDAWorkstationSetup_2308.exe"`.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

To set VDAs to upgrade from a local file share using PowerShell, use the `-VdaWorkstationPackageUri` (single-session OS) or `-VdaServerPackageUri` (multi-session OS) parameter when scheduling your upgrade.

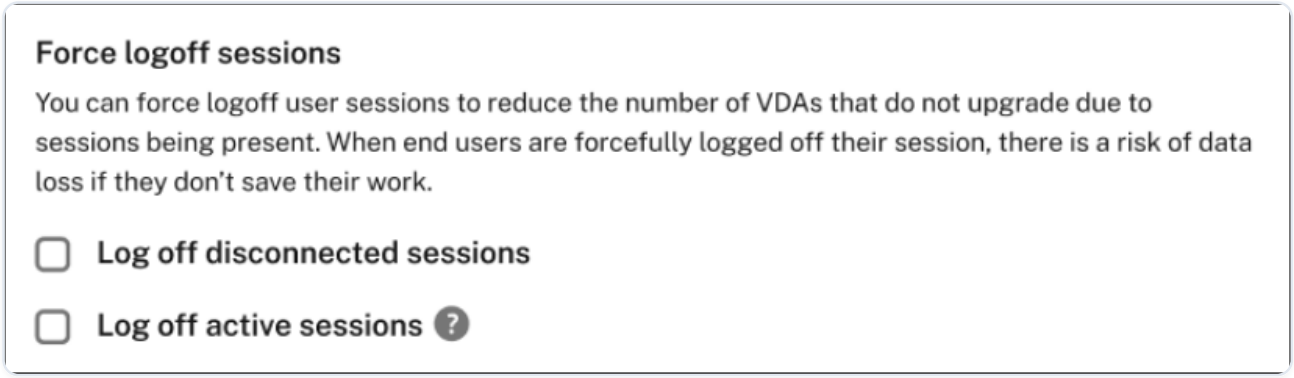
Force Logoff Sessions

To increase the number of VDAs that are available for upgrade during a scheduled upgrade, consider forcefully logging off user sessions during the upgrade. The forceful logoff occurs when the upgrade begins for each individual VDA, not at the start of the overall scheduled upgrade window.

Since different VDAs start upgrading at different times within the scheduled period, users will only be logged off when their specific VDA starts its upgrade.

To forcefully log off disconnected sessions during scheduled upgrades using the Full Configuration interface, select the **Log off disconnected sessions** option.

To forcefully log off active sessions during scheduled upgrades using the Full Configuration interface, select the **Log off active sessions** option. If logging off active sessions, users will receive a notification in their session 10 minutes before the upgrade starts, reminding them to save their work before being logged off automatically.



To forcesfully log off disconnected sessions during scheduled upgrades using PowerShell, use the `-LogoffOption` parameter when scheduling your upgrade. The available options for `-LogoffOption` are listed below:

- **ActiveSessionsOnly:** If an active session is on the VDA during the scheduled upgrade window, the user will be logged off. A banner will display 10 minutes before the user is logged off to provide a warning. VDAs with disconnected sessions will not be logged off during the upgrade window. If the disconnected session remains throughout the upgrade window, that VDA upgrade will be cancelled.
- **DisconnectedSessionsOnly:** If a disconnected session is present on the VDA during the scheduled upgrade window, the user will be logged off. Users are not notified that their

© 1997–2026 Citrix Systems, Inc. All rights reserved.

disconnected session will be logged off. VDAs with active sessions will not be logged off during the upgrade window. If the active session remains throughout the upgrade window, that VDA upgrade will be cancelled.

- **ActiveAndDisconnectedSessions:** If a disconnected or active session is on the VDA during the scheduled upgrade window, the user will be logged off. For active sessions, a banner will display 10 minutes before the user is logged off to provide a warning.
- **DoNotLogoff:** Active and disconnected sessions are not logged off. If a session is present on the VDA throughout the duration of the upgrade schedule, the upgrade is cancelled at the end of the scheduled upgrade window.

When possible, Citrix recommends forcefully logging off sessions to increase the number of VDAs that upgrade successfully.

IMPORTANT:

Forcefully logging off sessions can result in users losing unsaved work from their session.

Restart VDAs before starting the upgrade

Use the option to automatically restart VDAs before upgrades to improve the success rate by ensuring each VDA starts the process in a clean, consistent state. Restart before upgrade can mitigate the risk of common failures, such as pending restarts, lingering processes, or incomplete system updates.

When this option is enabled, each VDA is restarted individually just before its upgrade begins, rather than at the start of the overall upgrade window.

To use the restart VDA before upgrade feature, the VDA upgrade agent must be version 7.44 (released with Citrix Virtual Apps and Desktops 2503) or later. VDAs with an earlier VDA Upgrade Agent version will upgrade without a restart.

Power on machines to upgrade VDA

When scheduling a VDA upgrade, you can configure VDA Upgrade Service to automatically power on machines that are currently off or in hibernation at the start of the upgrade window.

By default, VDA Upgrade Service only upgrades machines that are powered on. Machines that are off or hibernated are skipped, which can leave part of your catalog running an older VDA version until the next upgrade window. Enabling this option ensures those machines are included in the upgrade run.

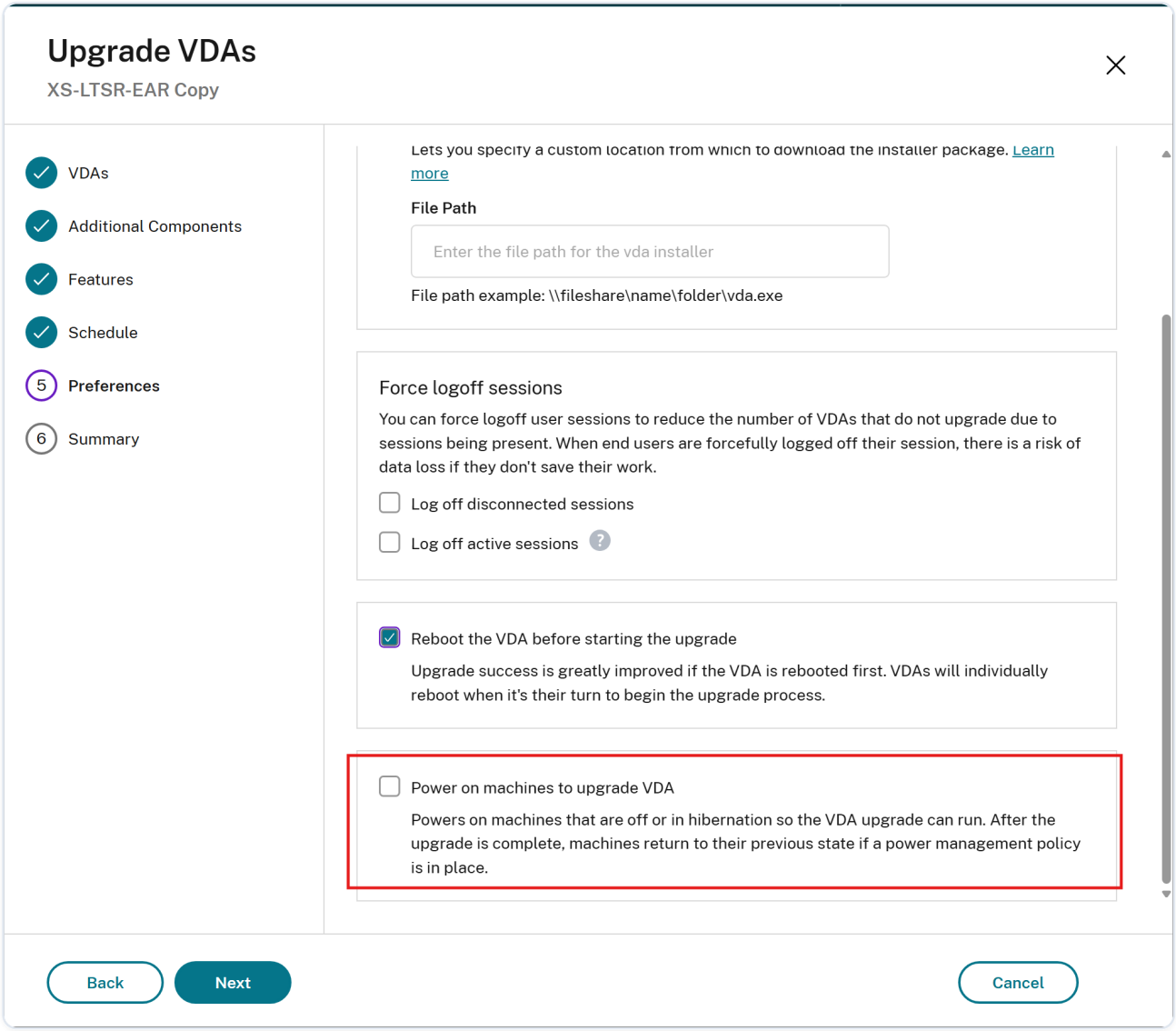
© 1997–2026 Citrix Systems, Inc. All rights reserved.

How it works

At the beginning of the upgrade window, VDA Upgrade Service powers on any machines in the scope of the schedule that are off or in hibernation, then upgrades them along with the rest of the catalog. When the upgrade completes, each machine returns to its previous power state — provided a power management policy is configured for the catalog or delivery group. The VDA upgrade service itself does not power off machines though.

To enable this option

When creating or editing an upgrade schedule in Studio, select Power on machines to upgrade VDA in the scheduling options before confirming the schedule.



NOTE:

Machines that are already powered on when the upgrade window starts are not affected by this setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Machines return to their pre-upgrade power state (off or hibernated) only if a power management policy is in place. If no policy is configured, machines remain powered on after the upgrade completes.
This option applies to both catalog-level and machine-level upgrade schedules.

Edit or Cancel the VDA workflow

After you schedule the upgrades for a catalog, you can edit the start time and duration of the upgrade or cancel it altogether.

To edit or cancel an upgrade using the UI at the machine catalog level, right-click on a machine catalog with an existing scheduled upgrade and click **Edit Scheduled VDA Upgrade**. To edit an existing machine catalog level upgrade using PowerShell, use the `Set-VusCatalogUpgrade` and `Remove-VusCatalogUpgrade` cmdlets.

To edit or cancel an upgrade at the machine level, in the search node, right-click on a machine with an existing scheduled upgrade and click **Edit Scheduled VDA Upgrade**. You cannot edit the scheduled VDA upgrade for multiple machines simultaneously. To edit an existing machine-level upgrade using PowerShell, use the `Set-VusMachineUpgrade` and `Remove-VusMachineUpgrade` cmdlets.

Monitor and Troubleshoot VUS

Monitoring Scheduled VDA Upgrades

VDAs and machine catalogs have two attributes to help monitor the readiness and current status of VDA upgrades that are visible as columns that can be used to filter in Studio or in the details pane of the VDAs or catalogs.

- VDA Upgrade
- VDA Upgrade State

VDA Upgrade

VDA Upgrade provides information on whether the VDA or machine catalog has the VDA upgrade agent configured and if VDAs are up to date or if an upgrade is available. The available statuses are as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA UPGRADE (STUDIO)	VDA UPGRADE (POWERSHELL)	DESCRIPTION
Catalog Level		
Not configured	MissingUpgradeType	An upgrade track (CR, LTSR, CR EAR, or LTSR EAR) has not been selected for the machine catalog.
Scheduled	UpgradeScheduled	An upgrade is scheduled for the machine catalog.
Available	UpgradeAvailable	VDAs in the catalog are not on the latest version of the upgrade track. An upgrade is recommended.
Up to date	UpToDate	VDAs in the catalog are on the latest version of the upgrade track. No action is required, or there is no available upgrade target that supports the VDA's current operating system.
Unknown	Unknown	Retrieving the latest VDA Upgrade state.
Machine Level		
Not configured	MissingUpgradeType	An upgrade track (CR, LTSR, CR EAR, or LTSR EAR) has not been selected for the machine catalog of the VDA.
Scheduled	UpgradeScheduled	An upgrade is scheduled for the VDA.
Available	UpgradeAvailable	The VDA is not on the latest version of the upgrade track. An upgrade is recommended.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA UPGRADE (STUDIO)	VDA UPGRADE (POWERSHELL)	DESCRIPTION
Up to date	UpToDate	The VDA is on the latest version of the upgrade track. No action is required, or there is no available upgrade target that supports the VDA's current operating system.
Checking state	Unknown	Retrieving the latest VDA Upgrade state.

NOTE:

- For VDAs using the LTSR track, a catalog will only show as Up to date if the VDAs are on the latest cumulative update (CU) of the latest long term service (LTSR) version. If the VDA is on the latest CU of a previous LTSR version, VDA Upgrade will still show as **Available**.
- A VDA also shows Up to date when no available upgrade target supports its current operating system (for example, Windows Server 2016 from CVAD 2407 onward). The Upgrade VDAs wizard then offers no target for the VDA. To upgrade it, re-image the machine to a supported operating system, then schedule the upgrade. See the System requirements for the target version and CTX224843.

VDA Upgrade State

VDA Upgrade State provides information on the status of a scheduled upgrade. The VDA Upgrade State statuses are as follows:

VDA UPGRADE STATE (STUDIO)	VDA UPGRADE STATE (POWERSHELL)	DESCRIPTION
Catalog Level		
Not scheduled	NotScheduled	No upgrade is scheduled for the catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA UPGRADE STATE (STUDIO)	VDA UPGRADE STATE (POWERSHELL)	DESCRIPTION
Scheduled	UpgradeScheduled	An upgrade is scheduled for the catalog.
In progress	UpgradeInProgress	An upgrade is in progress for the catalog.
Canceled	UpgradeCancelled	An upgrade was cancelled for the catalog. This can be due to a manual cancellation or the failure threshold being reached.
Failed	UpgradeFailed	A scheduled upgrade for the catalog failed.
Successful	UpgradeSuccessful	A scheduled upgrade for the catalog completed successfully. Note: A successful upgrade does not mean all VDAs in the catalog upgraded successfully.
-	Empty	No upgrade scheduled for the catalog.
Machine Level		
Scheduled	UpgradeScheduled	An upgrade is scheduled for the VDA.
Awaiting upgrade	UpgradeInUpgradeWindow	A scheduled upgrade is active, but the VDA has not started to upgrade yet. See “Concurrency” for more information on how VDA upgrades are load-balanced.
In progress	UpgradeInProgress	The VDA is currently upgrading.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA UPGRADE STATE (STUDIO)	VDA UPGRADE STATE (POWERSHELL)	DESCRIPTION
Canceled	UpgradeCancelled	A scheduled upgrade has been cancelled for the VDA before the upgrade began.
Upgrade failed	UpgradeFailed	The VDA began to upgrade but the upgrade failed to complete successfully. See “troubleshooting” for more information.
Succesful	UpgradeSuccess	The VDA upgraded successfully.
Validation failed	UpgradeValidationFailed	Certificate validation failed while downloading the metadata for the VDA installer.
-	Empty	No upgrade is scheduled for the VDA.

Troubleshooting Scheduled VDA Upgrades

If you encounter upgrade failures, the following logs can help you identify and troubleshoot the issues. You can also share these logs with Citrix Technical Support to expedite the assistance process.

VDA Installation Logs

When troubleshooting upgrade failures, gather and review the logs for both the initial installation of the VDA and the failed upgrade. Logs for installation and upgrades can be found in the following locations.

- Installation logs for VDA installations are placed in:
  - %temp%/Citrix/XenDesktop Installer
- Upgrade logs for VDA installations are placed either in:
  - C:\Windows\Temp\Citrix\XenDesktop Installer **or**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- C:\Windows\SystemTemp\Citrix\XenDesktop Installer

VDA Upgrade Agent Version

When gathering data to troubleshoot upgrade failures through VUS, it is important to know the version of the upgrade agent on the VDAs. To check VDA Upgrade Agent versions, use the following cmdlet: `Get-VusComponentVersion -ComponentType VUS`. It lists all VDAs and their VDA Upgrade Agent versions.

To check VDA Upgrade Agent versions at a catalog level, you can use the following script:

NOTE:

The script is intended as an example and might need to be adapted to suit your specific environment. We recommend that you test the script thoroughly before using it in a production environment.

```
Param( [Parameter (Mandatory=$true)] [string] $CatalogName ) try { $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-Object -Property UUID if($Uuids -eq $null) { throw "Cannot find CatalogName " +$CatalogName } Write-Output("Catalog Name passed is "+$CatalogName) foreach($Uuid in $Uuids) { $compVersion = Get-VusComponentVersion -MachineId $machine.UUID -ComponentType VUS $Machine = Get-BrokerMachine -UUID $compVersion.MachineId Write-Output(“MachineName: “+$Machine.MachineName+”, Machine UUID:”+$machine.MachineId+”, VUA Version:”+$compVersion.Version) } } catch { Write-Output(“Exception Occured”) Write-Host $_ }
```

Logs related to the VDA Upgrade Agent

VDA Upgrade Agent (VUA) logs can provide essential information for troubleshooting upgrade failures and issues with the VUA communicating with the VDA upgrade service. Logs you can collect include:

- Citrix Diagnostic Facility (CDF) traces. The CDF module name is VdaUpgradeAgent.
- Windows event logs. View logs in the Event Viewer > Windows Logs > Applications > Citrix VDA Upgrade Agent Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For VUA versions 7.44 and later

In the VDA Upgrade Service Agent version 7.44 (included in the 2503 release), a registry setting is available that allows administrators to enable a rotating log file that captures critical information for troubleshooting while preventing the log files from growing too large. The total size of log files is capped at 20 MB. Create the following registry key to enable logging to a file:

- **Key:**

  `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent -Name LogToFile -Value 1 -PropertyType DWord -Force`
- **Value name:** `LogToFile`
- **Value type:** `REG_DWORD`
- **Value data:**
  - `0` - file tracing disabled
  - `1` - file tracing enabled

To create the LogToFile registry key on a VDA using PowerShell, use the following cmdlet:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent -Name LogToFile -Value 1 -PropertyType DWord -Force
```

To enable LogToFile for groups of machines at scale, consider creating the LogToFile registry on all VDA organizational units (OUs) through Group Policy Preference.

NOTE:

- When `LogToFile=1` is set, logs are written only to the file. They will not appear in the CDF traces.
- The VDA Upgrade Agent service restart is required for the registry change to take effect
- The log file is created in C:\ProgramData\Citrix\Update Services\Logs folder

For VUA versions before 7.43

If needed, you can modify the VDA Upgrade Agent configuration file so that the logs are continuously written to a file. To enable logging to a file, follow these steps:

1. Go to the folder `C:\Program Files\Citrix\CitrixUpgradeAgent`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Open the file `Citrix.UpdateServices.UpdateAgent.exe.config`.
3. Change the value of `LogToFile` to `1`.
4. Restart the Citrix VDA Upgrade Agent service. This creates a log file at: `C:\ProgramData\Citrix\Update Services\Logs`.

NOTE:

- Enabling logging to a file through the .config file continuously writes logs, potentially consuming storage space. Remember to disable logging after the issue is resolved. To disable logging, first set `LogToFile` to `0` and then restart the Citrix VDA Upgrade Agent Service.
- When `LogToFile`=`1` is set, logs are written only to the file. They will not appear in the CDF traces.

Troubleshoot VDA upgrade download failures

Follow the steps below to troubleshoot and resolve download failures related to the VDA upgrade feature:

1. Make sure that relevant URLs have been added to the allow list if URL filtering is in place. See VDA upgrade requirement.
2. After adding the necessary URLs to the allow list, try rescheduling the VDA upgrade.

You can enable CDF tracing or set `LogToFile` to `1` to capture detailed logs for analysis. If the download failure issue persists, check the errors. If you see the following error message "Download Failed: This access control list is not in canonical form and therefore cannot be modified," it indicates that the permissions on the folder `C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA` are incorrect.

To address the issue, do either of the following:

- **Option 1:** Reset access control lists (ACLs) on the folder using the following command. (The command reset the ACLs with default inherited ACLs for all matching files.)
  - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA" /reset /T /C /L /Q
- **Option 2:** Delete the VDA folder under Downloads and then schedule the VDA upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot VDA upgrade validation failures

Follow the steps below to troubleshoot and resolve download failures related to the VDA upgrade feature:

1. Make sure that relevant URLs have been added to the allow list if URL filtering is in place, especially the Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) URLs needed for the revocation check. See VDA upgrade requirement.
2. After adding the necessary URLs to the allow list, try rescheduling the VDA upgrade.

We suggest enabling CDF tracing or setting LogToFile to 1 to capture detailed logs for analysis. The logs can include the following errors:

- RevocationStatusUnknown
- The revocation function was unable to check the revocation status for the certificate.
- The revocation function was unable to check revocation because the revocation server was offline.

The VDA Upgrade Agent relies on Windows system calls to validate certificates and perform revocation checks. The errors above indicate that the agent is unable to establish a connection to the CRL or OCSP URLs.

The Windows CryptoAPI does not currently support proxy settings. Review the VDAs with Proxy configurations section for configuring your VDA proxies to facilitate outbound CRL calls.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix DaaS™ for Citrix Service Providers

This article describes how **Citrix Service Providers** (CSPs) can set up and manage *multitenant* Citrix DaaS environments in Citrix Cloud. It also explains how tenant customers can access and co-manage their assigned environments through delegated administration.

For an overview of the features available for Citrix Partners, see Citrix Cloud for Partners.

The setup and management process involves two key areas:

- Manage multitenant DaaS deployments as partner administrators: How CSPs (Partners) configure and manage multitenant DaaS environments in Citrix Cloud.
- Manage your DaaS resources as tenant administrators: How tenant customers access and manage their own DaaS resources in cooperation with CSPs under multitenant deployments.

Requirements

- To set up and manage a multitenant Citrix DaaS environment in Citrix Cloud™, **Partners** must meet the following prerequisites:
  - Have Citrix Service Provider partner status
  - Have a Citrix Cloud™ account.
  - Have an active multitenant Citrix DaaS subscription
- To manage a tenant's DaaS resources in a multitenant Citrix DaaS environment, **Tenant administrators** must meet the following prerequisites:
  - Have Citrix Cloud account created by a CSP and added to the CSP's multitenant DaaS service
  - Be assigned a tenant DaaS administrator role

Limitations

This section outlines the current limitations in the CSP multitenant DaaS environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Tenant administrators can create and update hosting connections only after the partner administrator assigns a zone to the tenant scope. Tenant administrators still cannot manage tags because tag objects aren't scoped.
- If a zone is assigned to the tenant scope, DaaS creates machine catalogs in that zone automatically. If no zone is assigned, the partner administrator must create the first machine catalog, assign it to a zone, and apply the appropriate scope in the partner's Studio console.
- Tenant administrators cannot access Workspace Environment Management™ (WEM) configuration sets. A partner administrator must assign the configuration set.
- Folders under **Machine catalogs** are not yet scoped so that aren't accessible to tenant administrators.

NOTE:

The partner Studio console doesn't automatically enforce scopes. You are responsible for selecting the appropriate scope when creating machine catalogs, delivery groups, and application groups for the appropriate tenant.

Partner service administration

This article describes how Citrix Service Providers (Partners) set up and manage *multitenant* DaaS environments in Citrix Cloud.

For more information about requirements for CSP partners, see Requirements.

NOTE:

To set up a single-tenant DaaS deployment and manage this customer's DaaS resources, follow the standard process described in the DaaS get-started guide.

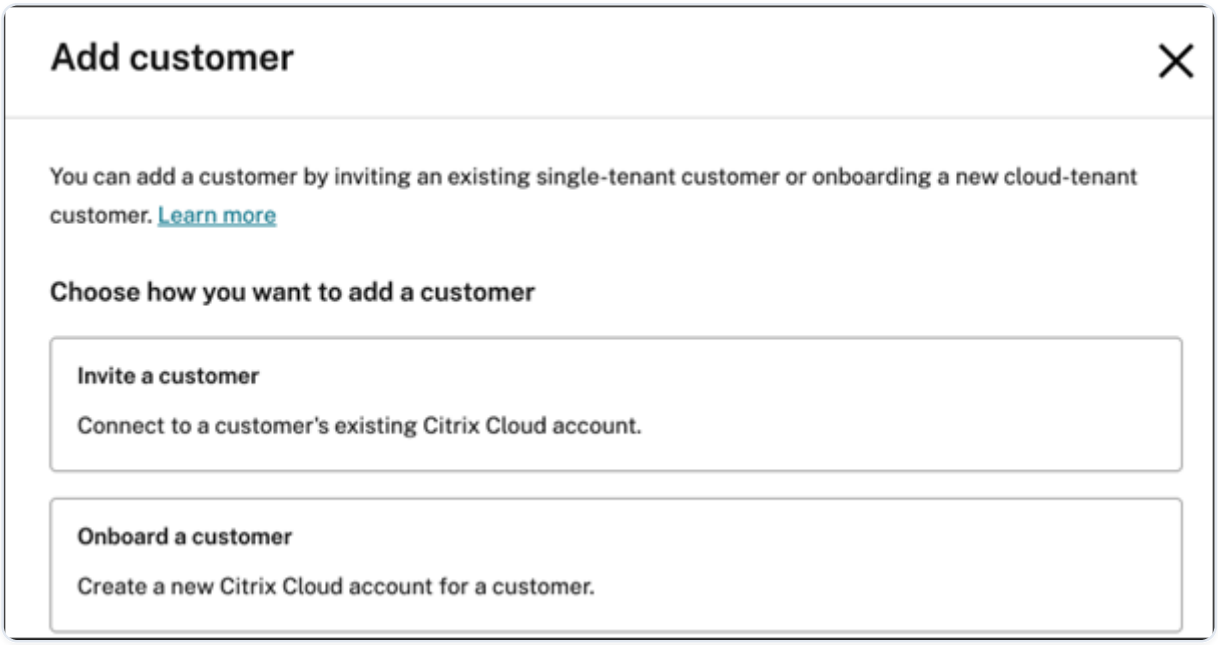
Step 1: Add a customer

Follow this procedure to onboard a *multitenant* customer that shares Org ID as the partner. The steps also apply to onboard a *single-tenant* that shares Org ID as the partner.

1. Sign in to Citrix Cloud with your Citrix Service Provider™ (CSP) credentials. Select **My Customers** in the upper left menu.
2. From the **My Customers** Dashboard, select the **Cloud-tenant** tab, click **Add customer**, and then choose **Onboard a customer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Complete the required fields and click **Add**.



NOTE:

Adding the customer creates a customer cloud account and automatically adds you (partner administrator) as a Full access administrator of that tenant.

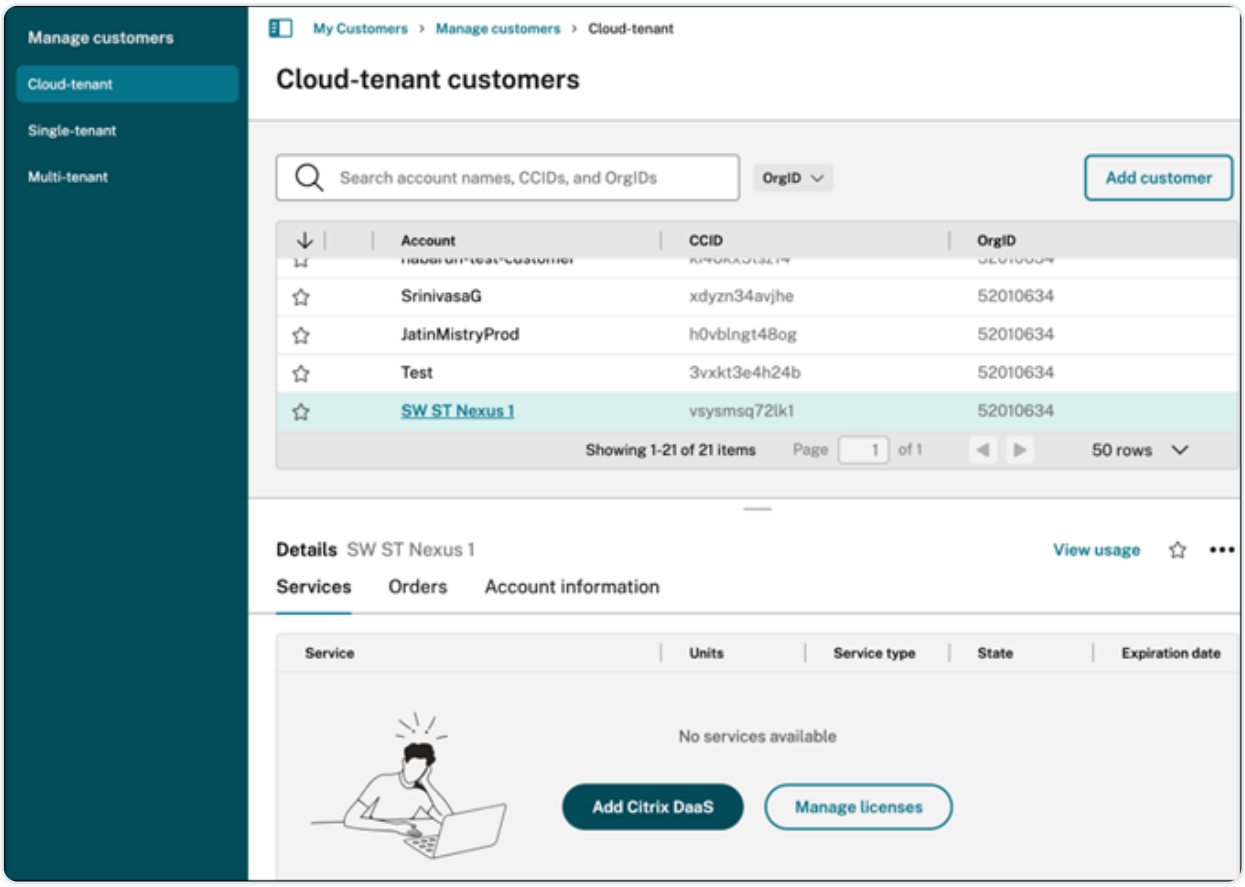
To Connect a *single-tenant* customer with an existing stand-alone Org ID and cloud account, follow these steps:

1. From the **My Customers** Dashboard, select the **Cloud-tenant** tab, click **Add customer**, and then choose **Invite a customer**.
2. Connect with an existing Citrix Cloud customer by sending the Citrix Cloud URL to the customer. For more information, see Create connections with customers. The customer must add you as a Full access administrator to their account. See Add administrators to a Citrix Cloud account for more information.

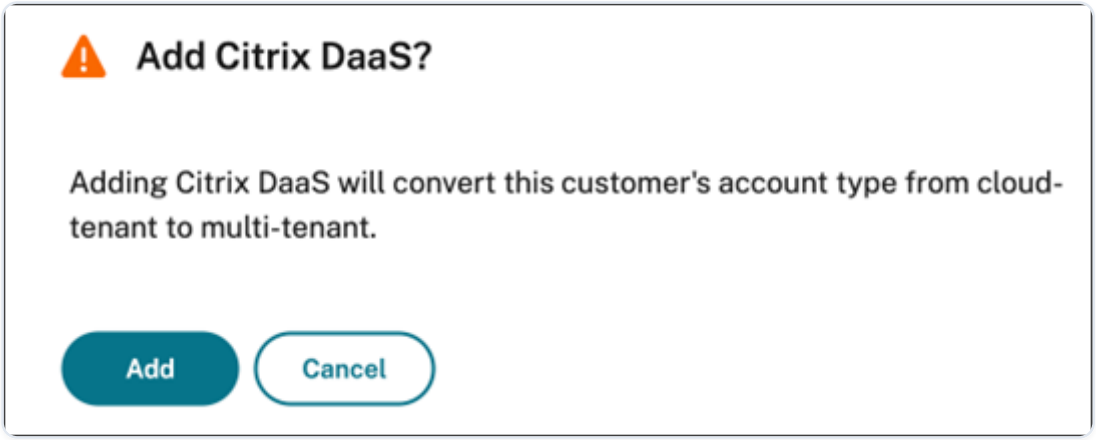
Step 2: Add Citrix® multitenant DaaS to a customer

1. Sign in to Citrix Cloud with your CSP credentials. Select **My Customers** in the upper left menu.
2. From **My Customers** dashboard, go to the **Cloud-tenant** tab, select the customer, and in the lower **Details** panel of the selected customer, click **Add Citrix DaaS**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **Add** to confirm.



TIP:

If the partner administrator cannot perform **Add DaaS** for a new tenant, verify that the following requirements are met:

- The signed-in administrator has Full access permissions in the tenant's Citrix Cloud account.
- The Citrix Service Provider account has the required multitenant Citrix DaaS entitlement.

After you complete this procedure, the customer is onboarded to your Citrix DaaS subscription.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When the onboarding completes, a new customer scope is created automatically in Citrix DaaS. The scope is visible in the Studio display. This scope is unique to that customer. You can rename the scope, but you cannot delete it.

Use this scope to tailor access for other administrators. For example, let's say you have 10 customers and two administrators. Using the unique scope, you can restrict one administrator's access to only three of the customers. The other administrator can access one of those three customers, plus two other customers. For details, see Control administrator access to customers.

Step 3: Set up a resource location

A resource location holds the machines that deliver apps and desktops for your customers, and infrastructure components such as Citrix Cloud Connectors. For details, see Connect to Citrix Cloud.

In multitenant DaaS deployments, tenants are separated by resource locations and their associated domains. Although each tenant has its own cloud account, all tenant resource locations and their cloud connectors must be deployed and managed from the CSP's partner account. For more information about detailed architecture and deployment options, see Citrix Service Provider DaaS Reference Architecture.

Step 4: Federate domains

Federated domains enable customer users to use credentials from a domain attached to your resource location designated to the tenant customer to sign in to their store. This behaviour allows you to provide dedicated stores to your customers that customer users can access using a custom store URL defined in the tenant account (*for example*, customer.cloud.com), while the resource location is still on your Citrix Cloud account. You can provide dedicated stores alongside the shared store that customers can access using your CSP store URL (*for example*, csppartner.cloud.com).

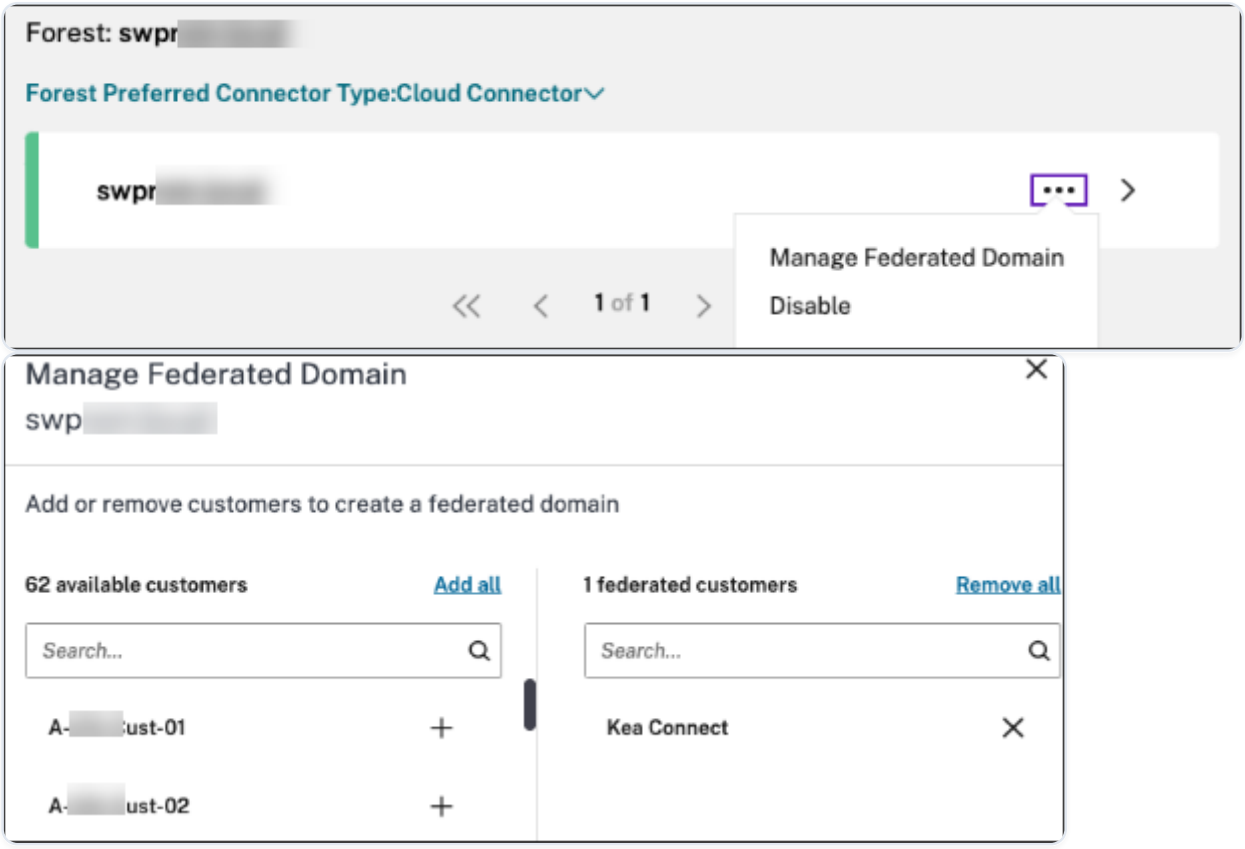
To enable customers to access their dedicated store, add them to the appropriate domains that you manage. After configuring the store through StoreFront Cloud, customers' users can sign in to their store and access the apps and desktops that you've made available.

Add a customer to a domain

1. Sign in to Citrix Cloud with your CSP credentials. Select **Identity and Access Management** in the upper left menu.
2. On the **Domains** tab, locate the relevant domain for the customer, and select **Manage Federated Domain** from the domain's ellipsis menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Manage Federated Domain** card, under the **Available customers** column, select the customer you want to add to the domain, and click the plus sign next to the customer name. The selected customer now appears in the **Federated customers** column. Repeat to add other customers. When you're done, select **Apply**.



Remove a customer from a domain

When you remove a customer from a domain that you manage, the customer's users can no longer access their stores using credentials from your domain.

1. From the Citrix Cloud menu, select **Identity and Access Management**, then select **Domains**.
2. Locate the domain that you want to manage and select the ellipsis button. Select **Manage Federated Domain**.
3. From the list of federated customers, locate or search for the customers you want to remove and select the X button. Select **Remove all** to remove all the customers in the list from the domain. The selected customers move to the list of available customers.
4. Select **Apply**.
5. Review the customers that you selected and select **Remove Customers**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 5: Assign a zone to tenant scope

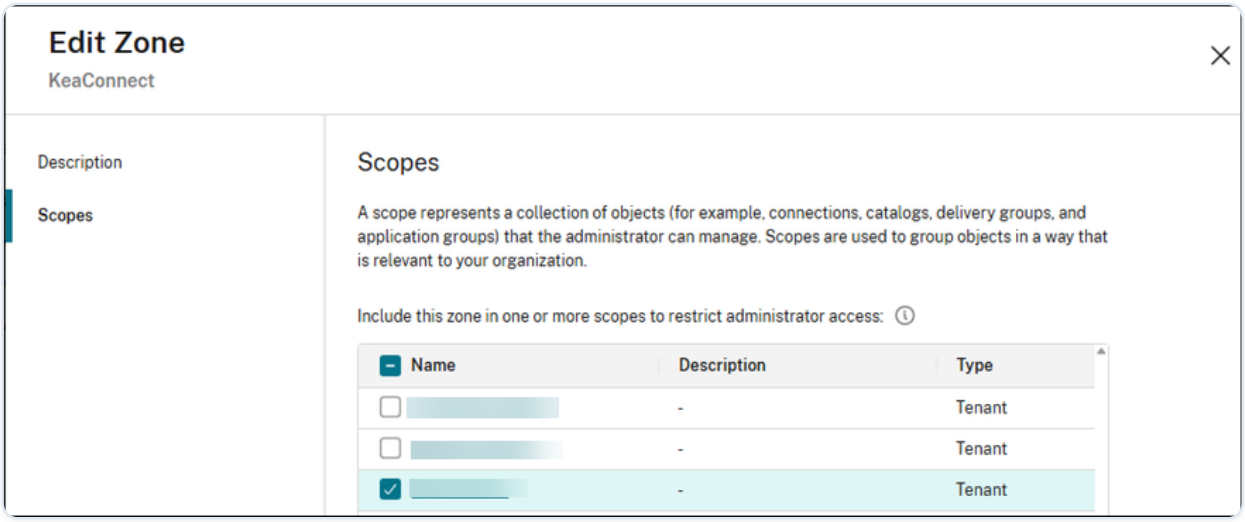
Zones can now be scoped to a tenant. After you assign a zone to a tenant's scope, the tenant administrator can manage their own hosting connections and machine catalogs within that zone. Assign the zone that corresponds to the resource location you set up for the tenant.

To assign a zone to a tenant's scope:

1. In the Citrix DaaS Studio console, go to **Manage > Zones**.
2. Select the zone whose name matches the tenant's resource location, and then select **Edit zone**.



3. On the **Scopes** tab, select the tenant's scope, and then select **Save**.



Step 6: Create a policy set for tenant scope

Tenant administrators can manage policies only within a policy set that you assign to their scope. To let a tenant manage policies independently, create a policy set and assign it to the tenant's scope. The tenant administrator can then create and manage policies within that policy set.

Policy sets are not enabled by default. To use this feature, first enable policy sets, and then create a policy set and assign it to the tenant scope.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 7: Set up catalogs and groups to deliver apps and desktops

NOTE:

To manage DaaS for a tenant customer as a partner administrator, you must switch to the CSP's cloud account. To do so, click the account name in the upper-right menu and click **Change customer**.

A catalog is a group of identical virtual machines. When you create a catalog, an image is used (with other settings) as a template for creating the machines. For details, see Create machine catalogs.

A delivery group is a collection of machines selected from one or more machine catalogs. The delivery group specifies which users can use those machines, plus the applications or desktops available to those users. For details, see Create delivery groups.

Application groups let you manage collections of applications. You can create application groups for applications shared across different delivery groups or used by a subset of users within delivery groups. For details, see Create application groups.

Machine catalogs and delivery groups for tenants can be created in two ways: the partner administrator creates them in the partner account and assigns them to the relevant tenant scopes, or tenant administrators create them from their own tenant cloud accounts.

When configuring groups, be sure that:

- The delivery group’s scope is a subset of the machine catalog’s scope. For example, assume the catalog’s scope is A and B. The delivery group’s scope can be either A or B, or A and B.
- The application group’s scope is a subset of the delivery group’s scope. For example, assume the delivery groups associated with an application group have scope A and B. The application group’s scope can be either A or B, or A and B.
- For security considerations in a multitenant deployment, it is recommended to separate all the preceding objects by specific tenant scopes.

NOTE:

The partner Studio console doesn’t automatically enforce scopes. You are responsible for selecting the appropriate scope when creating machine catalogs, delivery groups, and application groups for the appropriate tenant.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 8: Control administrator access to customers

You can control administrator access to customers by using the unique scope that was created when you added Citrix DaaS to the customer. You can configure access when you add an administrator or later.

To learn about restricting access using roles and scopes in Citrix DaaS, see Delegated administration.

Add a partner administrator with restricted access

1. Sign in to Citrix Cloud with your CSP credentials and select your partner account from the available accounts list.
2. Select **Identity and Access Management** in the upper left menu.
3. On the **Administrators** tab, select **Add Administrators From**, and then select **Citrix Identity**.
4. Type the email address of the person that you're adding as an administrator, and then select **Invite**.
5. Configure the appropriate access permissions for the administrator. Citrix recommends selecting **Custom access**, unless you want the administrator to have management control of Citrix Cloud and all subscribed services.
6. After selecting **Custom access**, select one or more role and scope pairs for Citrix DaaS, as needed. Be sure to enable only entries that contain the unique scope that was created for the customer.
7. When you're done selecting role and scope pairs, select **Send Invite**.

When the administrator accepts the invitation, they have the access that you assigned.

Edit delegated administration permissions for administrators

1. Sign in to Citrix Cloud with your CSP credentials and select your partner account from the available accounts list.
2. Select **Identity and Access Management** in the upper left menu.
3. On the **Administrators** tab, select **Edit Access** from the ellipsis menu for the administrator.
4. Select and clear role and scope pairs for Citrix DaaS, as needed. Be sure to enable only entries that contain the unique scope that was created for the customer.
5. Select **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View DaaS administrators and their assigned roles and scopes

1. Sign in to your Citrix Cloud partner account with your CSP credentials.
2. Select the **DaaS** tile in the upper left menu.
3. Select **Administrators** in the left pane.

Information is available on three tabs:

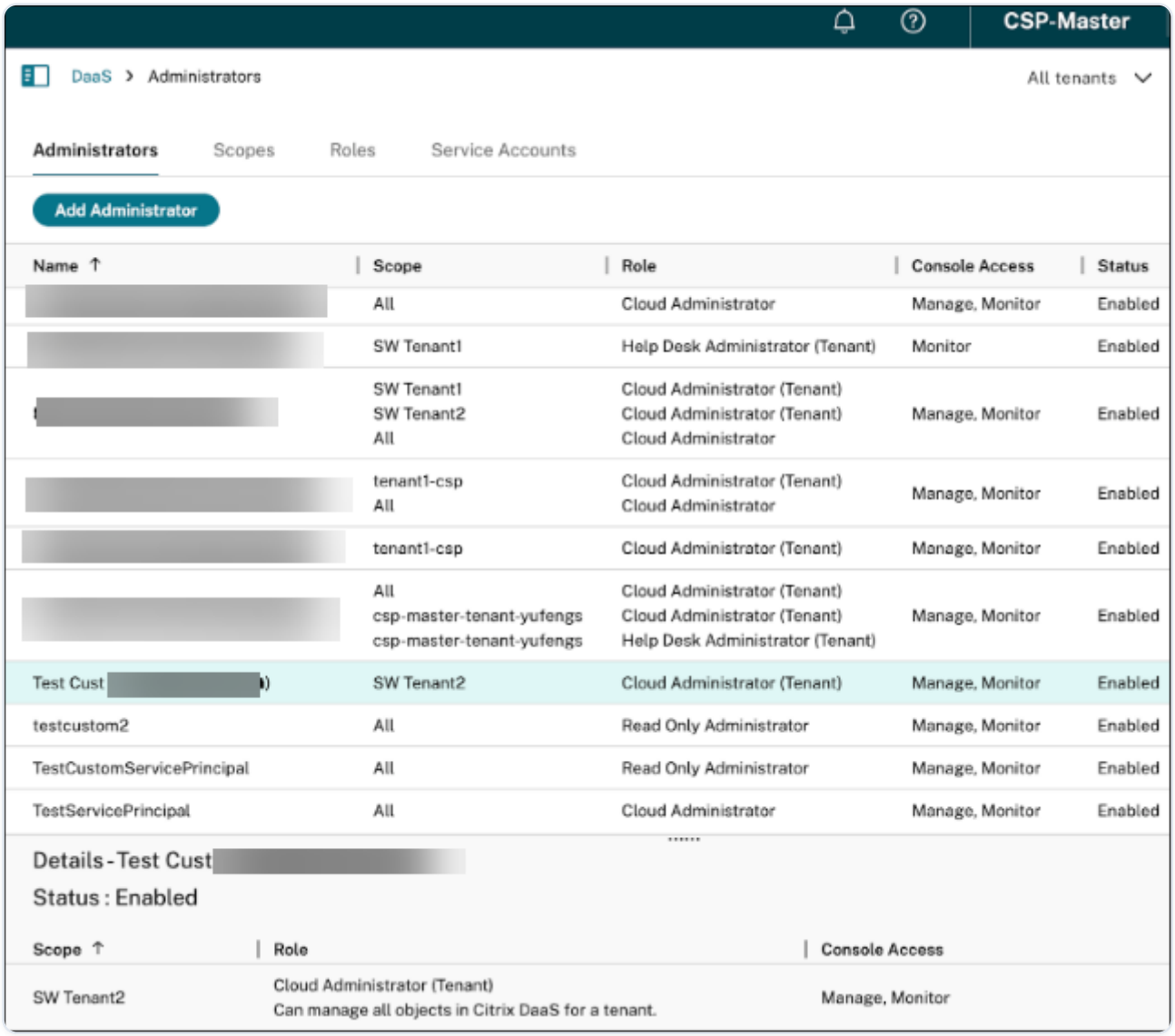
- The **Administrators** tab lists the administrators that have been created, plus their roles and scopes.
- The **Roles** tab lists all roles. To view role details, select the role in the middle pane. The lower portion of that pane lists the object types and associated permissions for the role. Select the **Administrators** tab in the lower pane to display a list of administrators who currently have this role.
- The **Scopes** tab lists all the scopes, including the scopes generated for customers of Citrix partners.

Export administrator activities for auditing

In a multitenant Citrix DaaS environment, multiple tenant customers share a DaaS instance. Each tenant has its own scoped administrative access. Gaining visibility into roles and scopes helps ensure secure delegation and simplifies auditing.

All tenant-level administrator roles defined in tenant accounts are automatically synced to the **Administrators** dashboard in the partner's Studio console. A partner administrator with **Full access** can export the data as a CSV file for reporting and analysis.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more auditing, the administrator activity history can also be exported from the **Logging** node in Studio.

Step 9: Configure stores

A customer can have its own store with a unique `customer.cloud.com` or custom URL defined in the customer's cloud account. This store is where the customer's users access their published apps and desktops. Alternatively, the CSP might share its partner branded store URL with various tenant customers.

To view or configure partner shared store URLs:

1. Sign in to your Citrix Cloud partner account with your CSP credentials.
2. Select **StoreFront Cloud** from the upper left menu.

You can change access and authentication to a store. You can also customize the store appearance and preferences. For details, see the following articles:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Customize your store experience
- Authentication

To view or configure a tenant customer’s store URL:

1. Sign in to the tenant customer’s Citrix Cloud account.
2. Go to **StoreFront Cloud**.

NOTE:

- For any authentication method used in the tenant account, the partner administrator must first enable the same method in the parent CSP account under **Identity and Access Management** before it can be configured in the tenant account.
- In scenarios where Citrix Federated Authentication Service (FAS) is deployed to process SSO for users in a multitenant environment, see the FAS multitenant support documentation for more information.

Monitor a customer's service

In a CSP environment, the **Monitor** dashboard functions the same as in a non-CSP environment, but displays multiple tenant scopes under the same DaaS instance. For more information, see Monitor for details.

By default, the **Monitor** dashboard displays data for all tenant customers. To view information for a specific tenant, select the tenant scope from the **All tenants** drop-down list in the upper-right corner.

Keep in mind that the ability of a partner administrator to see Monitor displays for a customer is controlled by the full administrator’s configured access. The access must include a role and scope pair that includes the customer’s unique scope.

If you used built-in roles to configure access: The built-in roles control whether the administrator can see the Studio displays. If you select only role and customer-scope pairs that don't include **Monitor** node visibility, that administrator cannot see the **Monitor** node for any selected customers. For example, if you give an administrator **Read Only Administrator,customerABC** access, that partner administrators cannot see the **Monitor** node for **customerABC**, because read only administrators cannot access Monitor displays.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

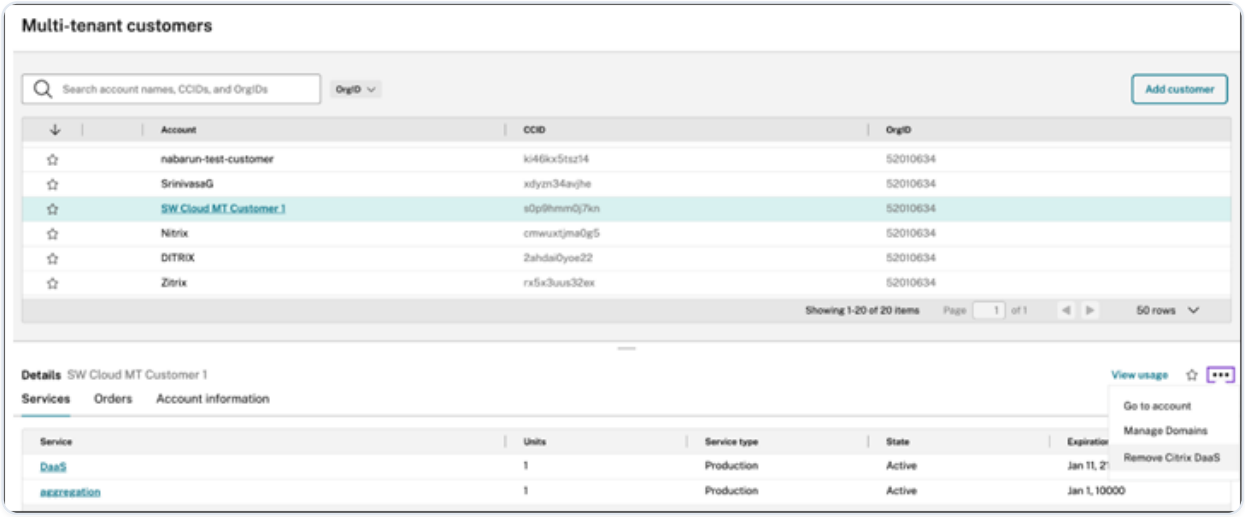
Remove the DaaS service from a customer

Prerequisites:

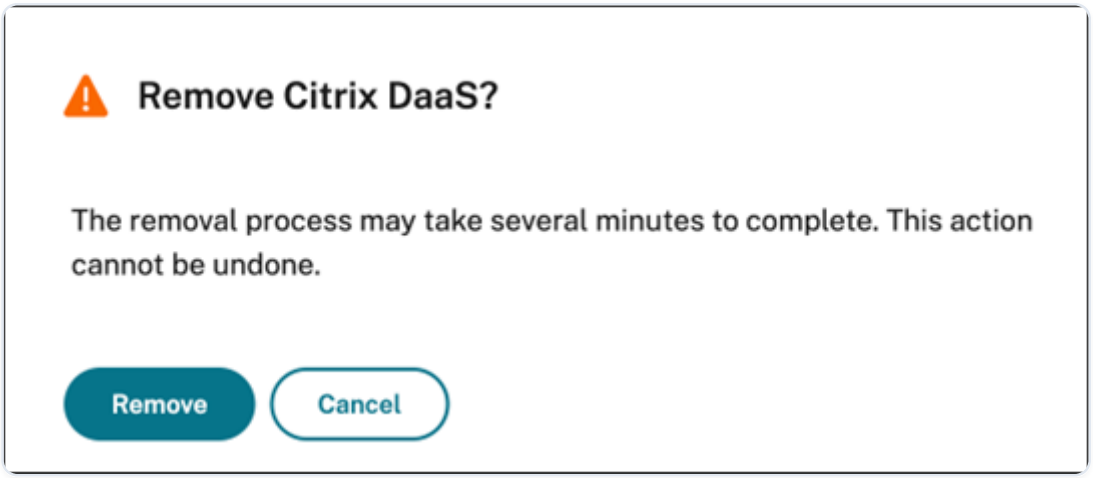
- Ensure that your customer scope is not linked to any Citrix DaaS objects. If they are linked, you cannot remove the service. To unlink scopes, go to **Studio > Administrators > Scopes** and edit the scope.
- To know your customer scope and manage it, see Create and manage scope.

To remove the DaaS service from a customer:

1. Sign in to your Citrix Cloud partner account with partner admin credentials with **Full access** permissions on the customer.
2. In the **My Customers** dashboard, go to the **Multi-tenant** tab, locate the customer, click the Ellipsis menu (…) next to the customer, and select **Remove Citrix DaaS**.



The following dialog box appears.



3. Click **Remove** to remove the service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Tenant service administration

This article describes how tenant customers access and manage their own DaaS resources in cooperation with Citrix Service Providers (CSPs) under *multitenant* deployment.

Add tenant administrators

In a multitenant environment, administrators of tenant customers must be added only in each tenant's Citrix Cloud account. Adding tenant administrators to the Citrix Service Provider's (CSP) partner account is *not* supported because it doesn't ensure proper security isolation.

The first tenant administrator must be added by a partner admin who initially created the tenant account. After that, this tenant administrator with Full access can add more tenant administrators.

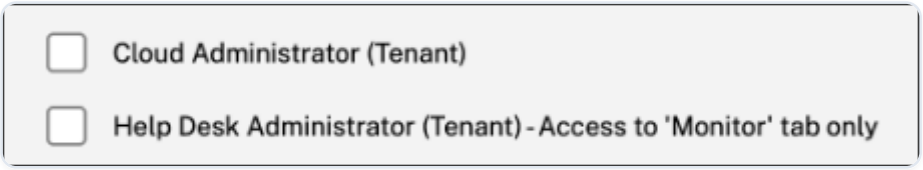
To add a tenant administrator:

1. Sign in to the tenant customer's Citrix Cloud™ account as a tenant administrator with **Full access** permission on the tenant.
2. Follow the steps in Invite individual administrators.
3. Assign one of the following permissions to the tenant administrator as needed:

   - **Cloud Administrator (Tenant)**: Has full permissions to manage the tenant's own machine catalogs, delivery groups, and other scoped objects. To assign this role, do one of the following:

     - Select **Full access**.
     - Select **Custom access**, then select **Cloud Administrator (Tenant)** under DaaS.

   - **Help Desk Administrator (Tenant):** Has access to the Monitor console only. To assign this role, select **Custom access**, then select **Help Desk Administrator (Tenant)** under DaaS.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

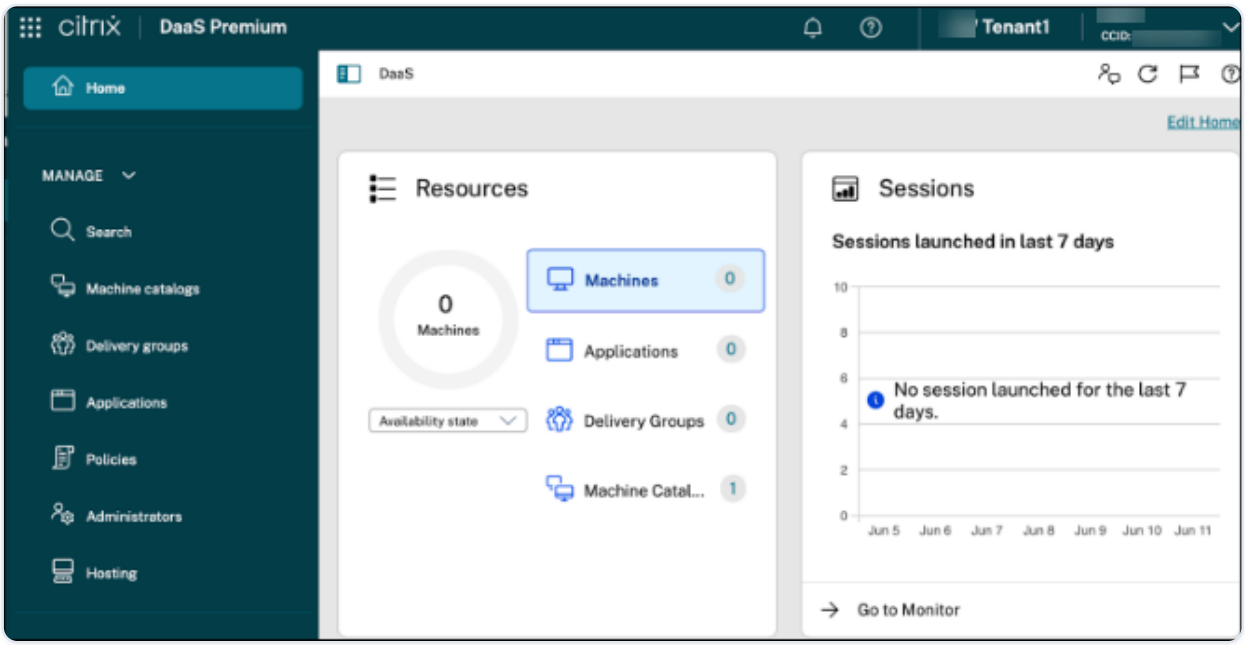
NOTE:

- Administrators added in the tenant account are automatically synced to the partner's Studio console with the appropriate role and scope.
- Partner administrators aren't encouraged to sign in to a tenant customer's cloud account for DaaS management. Certain features are blocked in tenant accounts for security reasons.
- To understand the permission differences between **Cloud Administrator (Tenant)** and **Help Desk Administrator (Tenant)**, see the following **Available features by tenant administrator role** table.

Access the Studio console in the tenant account

As a tenant administrator, you can access a scoped Studio experience directly from the tenant customer's Citrix Cloud account.

1. Sign in to the tenant customer's Citrix Cloud account.
2. Select **DaaS** from the home page or from the upper-left menu. The Studio console opens with functionality based on the administrator's assigned role.



The console displays only objects and settings within the tenant's scope. Unscoped objects are not accessible from the tenant view.

Table: Available features by tenant administrator role

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FUNCTION	CLOUD ADMINISTRATOR (TENANT)	HELP DESK ADMINISTRATOR (TENANT)
Home	Yes	Not applicable
Search	Yes	Yes
Machine Catalogs	Yes	Not applicable
Delivery Groups	Yes	Not applicable
Applications	Yes	Not applicable
Policies	Manage custom policy sets only	Not applicable
Administrators	Yes	Not applicable
Hosting	Yes	Not applicable
Monitor	Yes	Yes
Session Recording	Yes	Not applicable
Downloads	Yes	Not applicable
Settings	My preferences only	Not appicable

Update host connections

After the partner administrator assigns a zone to your tenant scope, you can create or update hosting connections within that zone as a tenant administrator with the **Cloud Administrator (Tenant)** role.

Create catalogs and delivery groups

As a tenant administrator with the **Cloud Administrator (Tenant)** role, you can manage machine catalogs and delivery groups within your assigned scope.

If the partner administrator assigns a zone to your scope, DaaS automatically creates all your machine catalogs in that zone. If no zone is assigned to your scope, the partner administrator must create the *first* machine catalog for your scope to ensure that the correct initial zone is selected for your catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage policies in the tenant account

By default, built-in policy sets are visible across all scopes in the partner's Studio console.

If a tenant needs to manage policies independently:

1. In the **partner account**, a partner administrator must create a **custom policy set** scoped to that tenant.
2. In the **tenant account**, tenant administrators with the **Cloud Administrator (tenant)** role manage policies within that set.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gateway

Citrix Gateway provides users with secure access to Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) applications.

The Citrix Gateway service enables secure, remote access to those applications, without having to deploy Citrix Gateway in the DMZ or reconfigure your firewall. The infrastructure overhead of using Citrix Gateway moves to Citrix Cloud.

For more information about the Citrix Gateway service, see the product documentation. That content includes how to enable the Citrix Gateway service and known issues for the version you're using.

Citrix ADC is an application delivery controller that analyses application-specific traffic to distribute, optimize, and secure Layer 4-Layer 7 (L4–L7) network traffic intelligently for web applications. The Citrix ADC VPX virtual appliance can be hosted on various virtualization and cloud platforms. For details, see Deploy a Citrix ADC VPX instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDKs and APIs

Citrix DaaS™ Remote PowerShell SDK

The Remote PowerShell SDK automates complex and repetitive tasks. It provides the mechanism to set up and manage the Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) environment without using Studio.

- Cmdlet details are provided in Citrix DaaS SDK.
- The supported modules are listed in Support and limitations. That section also lists the cmdlets that are disabled in this SDK.
- Remote PowerShell SDK is available for download in the Citrix website.

This product supports PowerShell versions 3 through 7.6.

How this SDK differs from the SDK for customer-managed deployments

In a Citrix Virtual Apps and Desktops deployment that is installed and managed by customer administrators, those administrators run cmdlets and scripts in a site containing VDAs and Delivery Controllers within a common domain structure. In contrast, Citrix DaaS splits the VDAs and Controllers into a resource location and the control plane, respectively. This split means that the original Citrix Virtual Apps and Desktops PowerShell SDK does not work in a Citrix DaaS environment. It cannot cross the secure boundary from the resource location to the control plane.

The solution is the Citrix DaaS Remote PowerShell SDK. When running in the resource location, the Remote PowerShell SDK accesses the control plane as if it is local. This provides the same functionality as a single Citrix Virtual Apps and Desktops site. There is only the lowest non-visible communication layer, enhanced to work either in a single local site or in the cloud environment. The cmdlets are the same, and most existing scripts remain unchanged.

The `Get-XdAuthentication` cmdlet provides the authorization to cross the secure resource location to control plane boundary. By default, `Get-XdAuthentication` prompts users for CAS credentials, and must be done once per PowerShell session. Alternatively, the user can define an authentication profile using an API-access Secure Client, created in the Citrix Cloud™ console. In both cases, the security information persists for use in subsequent PowerShell SDK calls. If this cmdlet is not explicitly run, it is called by the first PowerShell SDK cmdlet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

To use the Citrix DaaS Remote PowerShell SDK, whitelist the following URLs:

Commercial

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

Japan

- `https://*.citrixcloud.jp`
- `https://*.citrixworkspacesapi.jp/[customerid]`
- `https://[customerid].apps.citrixworkspacesapi.jp:443`

Government

- `hhttps://*.cloud.us`
- `https://*.citrixworkspacesapi.us/[customerid]`
- `https://[customerid].xendesktop.us:443`

Install and use the Remote PowerShell SDK

Requirements and considerations:

NOTE:

Do not install the Remote PowerShell SDK on a Citrix Cloud Connector™ machine. It can be installed on any domain-joined machine within the same resource location.

Citrix® does not support running this SDK's cmdlets on Cloud Connectors. The SDK's operation does not involve the Cloud Connectors.
If you also have a Citrix Virtual Apps and Desktops deployment (in addition to Citrix DaaS), do not install the Remote PowerShell SDK on an on-premises Delivery Controller. Because Citrix Studio (MMC-based) is installed as part of the Delivery Controller, you also cannot install the SDK on a server running Citrix Studio.

- Install **Microsoft Edge WebView2**.
- Ensure that PowerShell 3.0, 4.0, 5.0, 6.0 or 7.0 is available on the machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The SDK installer downloads and installs .NET Framework 4.8 if it (or a later supported version) is not already installed.
- If the machine already has the Citrix Virtual Apps and Desktops SDK installed, remove that SDK (from Windows Programs and Features) before installing the Remote PowerShell SDK.
- For an automated environment, use the `-quiet` parameter to install the SDK without user input.

To install the Remote PowerShell SDK:

1. From the download page, download the Virtual Apps and Desktops Remote PowerShell SDK.
2. Install and run the SDK.

Installation logs are created in `%TEMP%\CitrixLogs\CitrixPoshSdk`. Logs can help resolve installation issues.

Run the SDK on a domain-joined computer within that resource location:

- Open a PowerShell command prompt. You do not need to run as an administrator.
- If you want to use the snap-in (rather than the module), add the snap-in using the `Add-PSSnapin` (or `asnp`) cmdlet.
- You can explicitly authenticate by using the `Get-XdAuthentication` cmdlet. Alternatively, run your first Remote PowerShell SDK command, which prompts you for the same authentication as `Get-XdAuthentication`. If you are using a proxy, you must authenticate to the proxy to be able to use the `Get-XdAuthentication` cmdlet. For more information, see Use the Remote PowerShell SDK with a proxy.
- To bypass the authentication prompt, you can use the `Set-XdCredentials` cmdlet to create a default authentication profile, using a Secure Client created in the Citrix Cloud console.
- Continue running PowerShell SDK cmdlets or PowerShell SDK automation scripts. See an example.

To uninstall the Remote PowerShell SDK, from the Windows feature for removing or changing programs, select **Citrix Virtual Apps and Desktops Remote PowerShell SDK**. Right-click and select **Uninstall**. Follow the dialog.

Use the Remote PowerShell SDK with a proxy

If you are using a proxy, you might be unable to use the `Get-xdAuthentication` cmdlet because of the proxy blocking the HTTP requests that the cmdlet makes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

There are two ways to authenticate to the proxy. You can either use the `ProxyUseDefault` parameter or the `ProxyUsername` and `ProxyPassword` parameters:

- The `ProxyUseDefault` parameter enables authentication to the proxy by using the default proxy credentials. For example:

```
Get-XdAuthentication -ProxyUseDefault
```

- The `ProxyUsername` and `ProxyPassword` parameters enable authentication to the proxy within the PowerShell session. For example:

```
$secureString = ConvertTo-SecureString -String "password" -AsPlainText
-Force



Get-XdAuthentication -ProxyUsername user1 -ProxyPassword $secureString
```

NOTE:

You get an error if you run a command with `XDHyp:\` in the remote PowerShell SDK. To resolve this issue:

1. Run a command with `Hyp`. For example: `Get-HypServiceStatus`
2. Run a command with `XDHyp:\`. For example: `Get-ChildItem XDHyp:\Connections\`

Example activities

Common activities include setting up machine catalogs, applications, and users. A sample script is shown below.

```
    $users = "xd.local\Domain Users"



    $TSVDACatalogName = "TSVDA"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    $TSVDADGName = "TSVDA"


    $TSVDAMachineName = "xd\ds-tsvda2"


    #Create TSVDA Catalog


    $brokerUsers = New-BrokerUser -Name $users


    $catalog = New-BrokerCatalog -Name $TSVDACatalogName -AllocationType
"Random" -Description $TSVDACatalogName -PersistUserChanges "OnLocal"
-ProvisioningType "Manual" -SessionSupport "MultiSession"
-MachinesArePhysical $true


    #Add TSVDA Machine to Catalog


    $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
-CatalogUid $catalog.uid


    #Create new desktops & applications delivery group


    $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
$TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession"
-DeliveryType DesktopsAndApps -Description $TSVDADGName


    #Create notepad application
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    New-BrokerApplication -ApplicationType HostedOnDesktop -Name "Notepad"
-CommandLineExecutable "notepad.exe" -DesktopGroup $dg



    #Assign users to desktops and applications



    New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
$dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName



    New-BrokerAccessPolicyRule -Name $TSVDADGName
-IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers
-DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")



    New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
$dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName



    #Add machine to delivery group



    Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
```

Support and limitations

The following operating systems are supported by the Remote PowerShell SDK:

- Windows 11
- Windows 10
- Windows 10 IoT Enterprise LTSC x32 2019
- Windows 10 IoT Enterprise LTSC x64 2019

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows 10 IoT Enterprise 21h1 x64
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

The following Citrix Virtual Apps and Desktops PowerShell modules are supported in this release:

- Broker
- Active Directory (AD) Identity
- Machine creation
- Configuration
- Configuration logging
- Host
- Delegated administration
- Analytics

For details about cmdlets, see Citrix Virtual Apps and Desktops SDK.

After authentication, remote access remains valid in the current PowerShell session for 24 hours. After that time, you must enter your credentials.

The Remote PowerShell SDK must be run on a computer within the resource location.

The following cmdlets are disabled in remote operations to maintain the integrity and security of the Citrix Cloud control plane.

Citrix.ADIdentity.Admin.V2:

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Set-AcctServiceMetadata
- Set-AcctADAccountUserCert
- Test-AcctDBConnection

Citrix.Analytics.Admin.V1:

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

Citrix.DelegatedAdmin.Admin.V1:

- Add-AdminRight
- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

Citrix.Broker.Admin.V2:

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- Get-BrokerController
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Update-BrokerBrokerLocalLeaseCache

Citrix.Configuration.Admin.V2:

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

Citrix.Host.Admin.V2:

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

Citrix.ConfigurationLogging.Admin.V1:

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

Citrix.MachineCreation.Admin.V2:

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceMetadata
- Test-ProvDBConnection

Citrix.EnvTest.Admin.V1:

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

Citrix.Monitor.Admin.V1:

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix.Storefront.Admin.V1:

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

Citrix DaaS discovery module for App-V packages and servers

Citrix DaaS can deliver applications contained in App-V packages to your endpoints using either of the following methods:

- Single admin management method (accessing packages from a network share)
- Dual admin management method (accessing packages from a Microsoft App-V Management Server)

The process of registering App-V packages, Microsoft App-V Management, and Publishing Servers with the Application Library using Citrix DaaS differs slightly from registering packages using an on-premises deployment. However, the process of assigning applications to users and launching them on a user's endpoint is identical.

The Citrix DaaS management console in Citrix Cloud cannot view files in a resource location. Also, it cannot directly discover App-V packages or Microsoft App-V servers in your infrastructure. The discovery module provides functions that discover App-V package information in your on-premises infrastructure and uploads the package information to your Citrix DaaS. Package information includes App-V packages, Microsoft App-V servers, and the apps that the packages contain.

The discovery module uses the Virtual Apps and Desktops Remote PowerShell SDK. It can discover package information from either a network share or a Microsoft App-V Management Server. You use the discovery module on a machine in your resource location.

Prerequisites for using the discovery module:

- Verify that PowerShell 3.0 or later is available on the machine.
- Verify that the Citrix Virtual Apps and Desktops Remote PowerShell SDK is installed on the machine.
- Verify that you have access to the network share containing the App-V packages.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Verify that you have access to the server where the Citrix Cloud Connectors are installed and the Microsoft App-V Management Server is hosted.

Add App-V packages to the Application Library in Citrix Cloud

The following procedure is valid for adding App-V packages from network shares (single admin management) and adding all published App-V packages from the Microsoft App-V Management Server (dual admin management). With the dual admin management method, you must manage the added App-V packages just as you do when using the single admin management method.

1. Download the discovery module from the Citrix DaaS downloads page `<https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html>`. Extract the zip file `Citrix.Cloud.AppLibrary.Admin.v1.psm1` to a convenient folder.

   NOTE:

   This file is also provided on the Citrix Virtual Apps and Desktops ISO in `Support\Tools\Scripts`. You can copy it locally or reference it directly from the CD drive.

2. Verify that the Virtual Apps and Desktops Remote PowerShell SDK is installed on your machine
3. Navigate to the folder containing the discovery module. In the PowerShell window, type the full path of the folder containing the discovery module and then press **Enter**.
4. Import the discovery module with the command `Import-Module. \Citrix.Cloud.AppLibrary.Admin.v1.psm1`.
5. Add the App-V packages to the Application Library in Citrix Cloud using either of the following methods.

   - To add App-V packages from a network share, run the PowerShell cmdlet: `Import-AppVPackageToCloud`.

     For example: `Import-AppVPackageToCloud –PackagePath \ \AppVSrv\share\Notepad++.appv`

     For cmdlet help, type `Get-Help Import-AppVPackageToCloud`.

   - To add App-V packages from a Microsoft App-V Management Server, run the PowerShell cmdlet: `Import-AppVPackagesFromManagementServerToCloud`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example: `Import-AppVPackagesFromManagementServerToCloud –ManagementSrvFQDN AppVMngSrv.domain.local`

For cmdlet help, type `Get-Help Import-AppVPackagesFromManagementServerToCloud`

This command imports all published App-V packages from the Microsoft App-V Management Server to Citrix Cloud.

After adding the App-V packages to Citrix Cloud, you must manage them as you do using the single admin management method.

6. Sign in to Citrix Cloud. Select the target customer. After the script runs successfully, the App-V packages are added to the Application Library in Citrix Cloud.

High-level PowerShell functions

The module contains the following high-level functions that you can call from your own PowerShell script:

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

  Discovers and uploads to Citrix DaaS all the information necessary to publish applications from a single App-V Package.

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

  Discovers the UNC paths of packages published by the Management Server and calls **Import-AppVPackageToCloud** for each one in turn.

  Packages discovered in this way are loaded to Citrix DaaS using the single admin management method. Citrix DaaS cannot deliver packages using the dual admin management method.

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Discovers Microsoft App-V Management and Publishing Servers and imports the content to the Application Library. This cmdlet imports all the packages managed using Microsoft App-V Management Server and related information. Servers can be added and removed through PowerShell.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This cmdlet adds App-V packages in dual admin mode. Only App-V packages that are published on the Microsoft App-V Management Server, and which have AD groups added, are imported. If you make changes to the Microsoft App-V Management Server, rerun this cmdlet to synchronize the Application Library with the Microsoft App-V Management Server.

- `Remove-AppVServerFromCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Removes the Microsoft App-V Management and Publishing Servers added to Application Library.

  This cmdlet removes the specified Microsoft App-V Management and Publishing Servers, plus all the associated App-V packages.

Run the discovery module for App-V packages and servers on a domain-joined computer within that resource location. Follow the guidance in Install and use the Remote PowerShell SDK to get started. Continue running PowerShell cmdlets or scripts. See the following examples.

Example activities

Import the Citrix DaaS App-V package discovery module.

```
import-module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

Loop through the App-V Package store directory and upload each package.

```
Get-ChildItem -Path "\\FileServer.domain.net\App-V Packages" -Filter
*.appv |

Foreach-Object{

    Import-AppVPackageToCloud -PackagePath $_.FullName

}
```

Discover and upload packages registered with a Microsoft App-V management server.

```
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN
AppVManagementServer.domain.net
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Discover Microsoft App-V Management and Publishing Servers and add the configuration to the Application Library. This also imports all the packages managed by the Microsoft App-V Management Server in dual admin mode.

```
Import-AppVDualAdminCloud -ManagementSrvUrl http://
AppVManagementServer.domain.net –PublishingServerUrl http://
AppVManagementServer.domain.net:8001
```

Read the PowerShell help documentation included in the module.

```
Get-Help Import-AppVPackageToCloud
```

Limitations

- You cannot discover App-V packages on your resource location infrastructure directly from the Citrix DaaS management console in Citrix Cloud. For more information on Citrix Cloud, see the Citrix Cloud documentation.
- Citrix DaaS management console in Citrix Cloud does not have a live connection to the Microsoft App-V Management server. Changes to Packages and other configuration in the Microsoft App-V Management server are not reflected in the Citrix DaaS management console until `Import-AppVDualAdminCloud` is rerun.

Monitor Service OData API

In addition to using the Monitor functions to display historical data, you can query data using the Monitor Service's API. Use the API to:

- Analyze historical trends for planning
- Perform detailed troubleshooting of connection and machine failures
- Extract information for feeding into other tools and processes; for example, using Microsoft Excel's PowerPivot tables to display the data in different ways
- Build a custom user interface on top of the data that the API provides

For details, see Monitor Service OData API. To access the Monitor Service API, see Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix DaaS APIs

For a comprehensive list of Citrix DaaS APIs, see Citrix DaaS APIs.

Disclaimer

This software / sample code is provided to you "AS IS" with no representations, warranties, or conditions of any kind. You may use, modify, and distribute it at your own risk. CITRIX DISCLAIMS ALL WARRANTIES WHATSOEVER, EXPRESS, IMPLIED, WRITTEN, ORAL OR STATUTORY, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. Without limiting the generality of the foregoing, you acknowledge and agree that (a) the software / sample code might exhibit errors, design flaws or other problems, possibly resulting in loss of data or damage to property; (b) it might not be possible to make the software / sample code fully functional; and (c) Citrix may, without notice or liability to you, cease to make available the current version and/or any future versions of the software / sample code. In no event must the software / code be used to support of ultra-hazardous activities, including but not limited to life support or blasting activities. NEITHER CITRIX NOR ITS AFFILIATES OR AGENTS WILL BE LIABLE, UNDER BREACH OF CONTRACT OR ANY OTHER THEORY OF LIABILITY, FOR ANY DAMAGES WHATSOEVER ARISING FROM USE OF THE SOFTWARE / SAMPLE CODE, INCLUDING WITHOUT LIMITATION DIRECT, SPECIAL, INCIDENTAL, PUNITIVE, CONSEQUENTIAL OR OTHER DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. You agree to indemnify and defend Citrix against any claims arising from your use, modification, or distribution of the code.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix DaaS™ document history

The following table describes important changes to the Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) product documentation. These changes can be in addition to items in What's new.

For document history until November 2024, see Pre-December 2024 Document History.

To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	TITLE	DESCRIPTION
19 Aug 2026	Feature	**Citrix Advisor: Scheduled runs and Home page widget**	Advisor now runs site checks automatically on a recurring weekly schedule and retains each generated report for up to 90 days. A new **Advisor** widget on the **Home** page summarizes recommendations by impact level and lets you filter them by category. Learn more
17 Aug 2026	Feature	**Scoped zones for CSP multitenant DaaS**	Partner administrators can now assign a zone to a tenant scope and create policy sets for a tenant scope, enabling tenant administrators to manage their own hosting connections and machine catalogs within the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			assigned zone. Learn more
30 Jul 2026	Feature	**Local Host Cache Visibility Tool**	Introduced the Local Host Cache (LHC) Real-time Visibility Tool, a PowerShell-based solution that provides visibility into Citrix Local Host Cache environments. You can discover Cloud Connectors, identify the elected leader during LHC mode, enable or disable forced outage mode, and query event logs to troubleshoot LHC behavior. Learn more
30 Jul 2026	Feature	**Machine catalog experience enhancements in Studio**	Studio now shows the configured naming scheme in machine catalog details and reorders the action bar by usage frequency. Learn more
15 Jul 2026	Feature	**Task Center: Recurring tab and enhanced task management**	Task Center now includes a Recurring tab for tasks scheduled to run periodically or in the future. From Task Center, you can search, filter, and take actions such as cancel, rerun, edit, or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			delete on both recent and recurring tasks. Learn more
15 Jul 2026	Feature	**Citrix Advisor: New checks for reliability, performance, and operational excellence**	Citrix Advisor now includes new environment checks that help improve reliability, performance, and operational excellence. These checks help you proactively identify issues and take corrective actions across StoreFront, machine maintenance, and Always On Tracing workflows. Learn more
15 Jul 2026	Feature	**Extend configuration log search to include low-level operation details**	You can now extend the search scope in the **Logging** section of **Web Studio** to include low-level operation details. This enhancement lets you search details such as machine name and VDI name for more targeted troubleshooting. Learn more
15 Jul 2026	Feature	**Exclude draining machines from**	You can now exclude machines that are draining due to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		Autoscale capacity buffer	scheduled restarts from the Autoscale capacity buffer calculation for multi-session OS delivery groups. This helps prevent over-provisioning by counting only machines that are fully available to accept new sessions. Learn more
15 Jul 2026	Feature	**Deep links from Citrix Aidrien to DaaS**	When you ask Citrix Aidrien about machines or sessions, responses now include deep links to the corresponding DaaS console view with search filters applied automatically. This lets you jump directly from a chat response to the relevant interface without manually navigating or rebuilding filters. Learn more
13 Jul 2026	Feature	**Scope support for zones**	You can now apply scope control to zones (known as resource locations in Citrix Cloud). Scope support extends existing scope control capabilities to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			zone objects. You can grant custom administrators scoped access to specific zones. Learn more
13 Jul 2026	Feature	**Set up BYOL separately after connecting your AWS account**	You can now connect an Amazon Web Services (AWS) account to Web Studio without configuring Bring Your Own License (BYOL) support during the account connection process. You can connect your account first, then configure BYOL support at any time by selecting **Set up BYOL** from the **Accounts** list or from the account detail panel. Learn more
13 Jul 2026	Feature	**Faster domain selection with search**	Finding Active Directory domains and organizational units (OUs) is now faster in Web Studio. During machine catalog creation, when you select **Create new Active Directory accounts**, you can search for a specific domain directly from the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			Location (domain) drop-down list instead of browsing the full list of trusted domains. Learn more
17 Jun 2026	Feature	**Access Citrix DaaS data in Aidrien**	Aidrien can retrieve and display Citrix DaaS environment data directly within the chat, allowing you to investigate issues and manage resources without leaving the conversation. Learn more
09 Jun 2026	Feature	**Improved bulk actions in Web Studio**	You can now select all items across all pages or only within the current page. This enhancement removes the previous 500-item limit for bulk operations on matched search results, improving administrative efficiency in large environments with thousands of VDAs or sessions. Learn more
21 May 2026	Feature	**Studio support for controlling the visibility of packaged applications**	With Studio, you can now control the visibility of a packaged application —on a desktop, on

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			Citrix Workspace > Apps, or both. Learn more
18 May 2026	Feature	**Support for Numecent Cloudpaging applications**	You can now discover and publish Numecent Cloudpaging apps using the **App packages** node in Web Studio. You can also store Numecent Cloudpaging application containers on a network file share and discover and deliver them to end users in Studio by specifying the file share path. Learn more
15 May 2026	Feature	**Task Center now available**	Task Center provides a centralized view of scheduled and recurring tasks in Studio, helping you track these task statuses: Scheduled, Completed, Failed, or About to run. Access Task Center by selecting the calendar icon in the upper-right corner of the Studio console. Learn more
13 May 2026	Feature	**Amazon WorkSpaces Core**	You can now configure MCS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		Managed Instances: Studio support for MCS I/O (MCSIO) write-back cache	Storage Optimization (MCSIO) write-back cache (WBC) settings directly in Citrix Studio when creating or editing machine catalogs for Amazon WorkSpaces Core Managed Instances. Learn more
12 May 2026	Feature	**Resource filtering**	The resource filtering feature lets you configure rules to control user access to resources across delivery groups. You can define the resource type (application, desktop, or both), apply tag restrictions, and set conditions for rule enforcement based on factors like network location and store connection context. To access the feature, go to **Delivery groups > Settings > Resource filter**. Learn more
29 Apr 2026	Feature	**Update BDM disks for Citrix Provisioning catalogs**	ou can now update Boot Device Management (BDM) disks for your Machine Creation Services (MCS)-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			provisioned Citrix Provisioning catalogs. The BDM disk update helps update the Citrix Provisioning server addresses, and UEFI firmware using Studio or PowerShell. It supports Azure, Nutanix AHV Prism Central, VMware, and XenServer environments. Learn more.
29 Apr 2026	Feature	**Update vDisk assignments for MCS-provisioned Citrix Provisioning catalogs**	You can now update vDisk assignments for existing MCS-provisioned Citrix Provisioning catalogs using Studio or PowerShell. You can list available vDisks and assign existing vDisks at the catalog level. This feature applies to Azure, Nutanix AHV Prism Central, VMware, and XenServer environments. Learn more.
29 Apr 2026	Feature	**Reset OS disk for persistent VMs in Nutanix AHV Prism Central**	With this feature, you can now reset OS disk for persistent VMs using the `Reset-ProvVMDisk` PowerShell

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			command in Nutanix AHV Prism Central environments. Learn more.
28 Apr 2026	Feature	**Citrix Advisor: New checks for security, reliability, performance, and operational excellence**	Citrix Advisor now includes new environment checks covering security, reliability, performance, and operational excellence for StoreFront, VDAs, and Active Directory. These enhancements help you proactively identify issues and take corrective actions. Learn more.
28 Apr 2026	Feature	**Granular dismissal for Citrix Advisor recommendations**	Citrix Advisor now supports dismissing specific affected items within a recommendation rather than dismissing the entire recommendation. Available for machine catalogs, delivery groups, application groups, and zones. Learn more.
28 Apr 2026	Feature	**Customize Advisor check rules**	You can now customize Advisor check rules for Cloud Connector hardware,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			unused resources, and GPO configuration for VDAs. Customized recommendations are labeled with **Customized** for easy identification. Learn more.
28 Apr 2026	Feature	**Control application package update behavior with Preferences**	New **Preferences** settings in the **Studio > Application Packages** workflow let you preserve user favorites, prevent unintended downgrades, and automatically remove obsolete packages during update checks. Learn more.
28 Apr 2026	Feature	**Add notes for power actions**	You can now add optional notes when performing power actions on machines and sessions. Notes are recorded in logs for auditing purposes and support machine and session actions such as start, shut down, restart, and log off. Learn more.
28 Apr 2026	Feature	**Cloud Connector visibility for VDAs**	You can now see which Cloud Connectors your VDAs are proxied

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			through in **Web Studio > Search** using the new **Cloud Connector** column and filter. Learn more.
27 Apr 2026	Feature	**Support for creating Citrix Provisioning catalogs in Red Hat OpenShift and Nutanix AHV Prism Central virtualization environments using Studio**	With Studio, you can now create Citrix Provisioning catalogs in Red Hat OpenShift and Nutanix AHV Prism Central virtualization environments. This feature simplifies the process, letting you perform provisioning and power management tasks entirely within Studio. Learn more.
24 Apr 2026	Feature	**Azure ZRS disk types for prepared images**	MCS in Azure now enables you to select Zone Redundant Storage (`ZRS`) disk types for prepared images with MCS image management. This enhancement provides greater flexibility in disk type selection and improves the resiliency of your MCS machine catalogs in Azure by ensuring higher availability for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			prepared image disks. Learn more.
24 Apr 2026	Feature	**Image management in Nutanix AHV Prism Central environments**	Image management functionality is now generally available for OpenShift virtualization environments. This implementation significantly reduces the storage and time costs, and simplifies the VM deployment and image update process. Currently, you can also PowerShell commands to achieve this goal. Learn more.
24 Apr 2026	Feature	**Amulet Hotkey CoreStation plug-in (Preview)**	With this feature, Citrix manages your Amulet Hotkey CoreStation workloads through a Amulet Hotkey CoreStation plugin. With this plug-in, you can create hosting connections to your Amulet Hotkey CoreStation enclosure, create catalogs, and power manage machines in the catalog using PowerShell commands. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
24 Apr 2026	Feature	**Support for creating MCSIO-enabled MCS machine catalogs of Amazon WorkSpaces Core Managed Instances**	You can now create MCSIO-enabled MCS catalogs to create MCSIO-enabled MCS machine catalogs of Amazon WorkSpaces Core Managed Instances to improve write IOPS by directing write operations to the write-back cache and to reduce the startup time when the persisting OS disk is enabled. Learn more.
24 Apr 2026	Feature	**Manage on-premises image replication**	With this enhancement, you can run PowerShell commands and replicate the image version instance to storage locations. This feature applies to on-premises hypervisors, including VMware, XenServer, and Nutanix AHV Prism Central environments. Learn more.
24 Apr 2026	Feature	**Azure SSD storage for ephemeral OS disks**	This feature enhances ephemeral OS disk performance in Azure by allowing you to select higher-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			tier SSD storage types. Now, you can use `StandardSSD_LRS` or `Premium_LRS` by setting the `StorageType` custom property when creating an MCS catalog. Learn more.
24 Apr 2026	Feature	**Enhance Azure backup SKU mix**	This update allows you to include both hibernate-capable and non-hibernate-capable SKUs in your backup configurations. Learn more.
24 Apr 2026	Feature	**Bypass Cloud Connectors for Amazon WorkSpaces Core API requests**	When using Amazon WorkSpaces Core Managed Instances, you can now configure host connections to bypass Citrix Cloud Connectors for AWS API requests. This allows MCS to communicate directly from the Delivery Controller to AWS services for provisioning and power management operations instead of routing through a proxy. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
24 Apr 2026	Feature	**Change Azure VM availability zones**	This enhancement allows you to modify the availability zone property for existing MCS provisioned VMs in Azure. Previously, this required recreation of the VM. This feature provides greater flexibility, especially for persistent virtual machines. Learn more.
24 Apr 2026	Feature	**Flexible billing for Amazon WorkSpaces Core Managed Instances**	You can now choose between Monthly (flat-rate) and Hourly (pay-as-you-go) billing models when provisioning Amazon WorkSpaces Core Managed instances using Citrix MCS. This flexibility allows you to optimize compute costs based on your specific workload requirements and usage patterns. Learn more.
22 Apr 2026	Feature	**Troubleshoot with Citrix Aidrien**.	You can now troubleshoot warnings and errors in Citrix DaaS using Citrix Aidrien. Aidrien analyzes issues in context and provides

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			guided insights to help you diagnose and resolve problems faster. Learn more.
18 Apr 2026	Feature	**AWS EC2: Share AWS prepared images across regions**	You can now share a prepared image from one region to one or more different regions within the same AWS account. This feature is available for AWS EC2 environments. Learn more.
18 Apr 2026	Feature	**AWS EC2: Provision workloads in AWS local zones**	You can now provision AWS EC2 workloads directly in AWS local zones. You can create a host connection with a hosting unit in a desired local zone and then provision VMs in that local zone. Learn more.
31 Mar 2026	Update	**Image Management**	Reorganized the image management articles. Learn more.
26 Mar 2026	Update	**Remote Broker Provider**	Updated the description of the Event Id 3001. Learn more.
23 Mar 2026	Feature	**Support for Entra ID extension attributes in MCS**	You can manage your MCS machine catalogs using Entra ID extension

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			attributes (ExtensionAttribute1-15). For this, prepare a Service Principal with `Device.ReadWrite.All` permission. You can create and update an MCS machine catalog with Entra ID extension attributes using only PowerShell commands currently. The feature is supported for both Microsoft Entra joined and Microsoft Entra hybrid joined identity types. Learn more.
23 Mar 2026	Feature	**Nutanix AHV Prism Central: Improve network configuration**	This enhancement improves network configuration for MCS catalogs on Nutanix AHV Prism Central host connections. You can now configure network settings by clearly distinguishing between Basic VLANs, Advanced VLANs, and Overlay networks, preventing errors that occurred when mixed types were previously listed together. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
23 Mar 2026	Feature	**Share prepared image versions across hosts in the same resource pool in XenServer**	You can now use the **Images** node to share image versions across hosts in the same resource pool in XenServer. This implementation ensures consistency and uniformity of images across different hosts, enhancing deployment flexibility and operational efficiency. Learn more.
13 Mar 2026	Feature	**Citrix Advisor: New reliability check**	Citrix Advisor now includes a new environment check with the recommendation **Enable service continuity for Citrix Workspace**. This check identifies when service continuity isn't enabled and provides guidance to help you enable it. Learn more.
11 Mar 2026	Feature	**Customize column layout in Search main views**	You can now reorder columns in Web Studio to better organize and group related information. Web Studio retains your column order

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			and width preferences, so your customized layout persists across sessions. Currently, this capability is supported in the main views in **Search**. Learn more.
09 Mar 2026	Feature	**Service Window**	The Service Window feature provides a capability to schedule and automate operations on MCS-provisioned VMs. This feature currently supports various operations such as Reset OS disk and hardware configuration changes using PowerShell. Learn more.
27 Feb 2026	Update	**New section: Migrate to the App-V Single Admin worflow**	Added a section, *Migrate from App-V full infrastructure to Single Admin workflow*. Learn more.
27 Feb 2026	Update	**New section: Troubleshoot App-V applications**	Added a section, *Troubleshoot App-V applications (Single Admin model)*. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
12 Feb 2026	Feature	**Backup VM configuration in AWS EC2**	Studio now enables you to define a list of backup EC2 instance types (“Backup SKUs” that can be On-demand or Spot instances) in AWS environments that Machine Creation Services (MCS) can fall back to in case of capacity-related issues. Learn more.
12 Feb 2026	Feature	**Support for Azure Extended Zones**	You can now provision workloads in Azure Extended Zones using MCS provisioning. Azure Extended Zones are small footprint extensions of major Azure regions. They provide lower latency and data residency for customers that are further from the main region location. Learn more.
12 Feb 2026	Feature	**Red Hat OpenShift: Citrix Provisioning catalog using MCS**	This enhancement adds support to the OpenShift Plug-in to provision Citrix Provisioning (PVS) catalogs using MCS. Learn more.
12 Feb 2026	Feature	**Enroll HPE Moonshot machines to**	You can now register your non-domain joined or Microsoft

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		machine catalogs using WebSocket	Entra joined VDAs on HPE Moonshot to machine catalogs using WebSocket. Learn more.
12 Feb 2026	Feature	**Support for VMware vVols in MCS**	You can now use VMware vVols with MCS on vSphere environments. Previously, creating MCS catalogs on vVols resulted in PBM errors. This update resolves that issue. Learn more.
12 Feb 2026	Feature	**Use WinHttp (netsh) proxy server settings for hosting connection**	This feature allows hosting connections to use the WinHttp (netsh) proxy server settings configured on the Citrix Cloud Connectors to be used with the hosting connection. Learn more.
12 Feb 2026	Feature	**Cross-account provisioning in Amazon Workspaces Core Managed Instances using PowerShell**	This feature uses VPC peering and cross-account access using IAM roles to make provisioning across different AWS accounts possible for enterprises managing multiple AWS accounts. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
12 Feb 2026	Feature	**Provision workloads in AWS local zones**	You can now share a prepared image from one region to one or more different regions within the same AWS account. When you share an image, the underlying AMI is copied along with its properties, such as encryption, hibernation, tags, and trusted launch. Learn more.
12 Feb 2026	Feature	**Amazon WorkSpaces Core Managed Instances: Share AWS prepared images across regions**	You can now share a prepared image from one region to one or more different regions within the same AWS account. When you share an image, the underlying AMI is copied along with its properties, such as encryption, hibernation, tags, and trusted launch. Learn more.
12 Feb 2026	Feature	**Expanded icon support**	When customizing icons for desktops and applications in Studio, you can now extract and use icons from `.exe` files, in addition to the previously

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			supported `.ico` format. Learn more.
12 Feb 2026	Feature	**Citrix Advisor: New checks for reliability, performance, security, and cost effiency**	Citrix Advisor now includes the following new environment checks that provide actionable recommendations to help improve security, reliability, performance, and operational excellence. Learn more.
10 Feb 2026	Feature	**Forward Always-on Tracing (AOT) logs to your log server**	In Web Studio, you can now forward Always-on Tracing (AOT) logs from Citrix components to a designated log server. This feature enables centralized troubleshooting and more effective monitoring of your Citrix environment. Learn more.
10 Feb 2026	Feature	**Migrate machine catalogs to Citrix-managed Nutanix AHV Prism Central host connection**	With this feature, you can migrate your Citrix machine catalogs, and their associated VMs from existing Nutanix AHV (for Prism Element) and Nutanix AHV PC (for NC2 on Azure) host connections to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			the Citrix-managed Nutanix AHV Prism Central host connection. Learn more.
05 Feb 2026	Feature	**Single-use pooled desktops during LHC events**	Power-managed, single-session, pooled desktops are now available for a single use by default during a Local Host Cache (LHC) event. This change ensures that users can access these machines without the concerns about desktop reuse. Learn more.
03 Feb 2026	Feature	**Use machine profiles for Nutanix AHV Prism Central host connections**	You can now use machine profiles to define hardware configurations for VMs provisioned through your Nutanix AHV Prism Central host connection. You can create a new catalog with a machine profile, update an existing catalog, and convert a non-machine profile based machine catalog to a machine profile based machine catalog using Studio. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
30 Jan 2026	Feature	**Discover and deliver Citrix elastic app layers in Studio**	You can now discover and deliver Citrix elastic app layers using the **App packages** node in Studio. Learn more.
30 Jan 2026	Feature	**In-session notifications for background operations**	Web Studio now includes a notification center that gives you real-time visibility into background operations and reports on operation results. Learn more.
21 Jan 2026	Feature	**Follow-me tagging**	Follow-me tagging enables tracking of individual end-user VM usage by applying hypervisor-level tags. These tags, labeled with the specific user and/or organization (using `citrix-user-upn` as the key and the User Principal Name (UPN) as the value), are added when a user is assigned to a VM and removed when the user is unassigned. Learn more.
14 Jan 2026	Feature	**Provision a data disk on MCS created VM**	With this feature, you can now create and assign a persistent data disk to an MCS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			created persistent or non-persistent VM of an MCS machine catalog in AWS. The source of the data disk must be the master image (AMI's secondary volume). You can provision the data disk using both Studio and PowerShell commands. Learn more.
19 Dec 2025	Feature	**Azure: Clone MCS catalogs**	You can now use the Copy-ProvScheme PowerShell command to clone an existing persistent and non-persistent MCS machine catalog in the Azure virtualization environment. This feature creates a new provisioning scheme by copying the details of an existing scheme, including associated configurations, network mappings, and security groups. Learn more.
09 Dec 2025	Feature	**Enhanced experience optimization settings for Citrix DaaS**	We've enhanced **Experience Optimization** settings to help you easily fine-tune

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			resource allocation and boost performance across machine catalogs. You can now create or select configuration sets for tailored optimization, or quickly apply default settings like automatic CPU spike protection and intelligent CPU optimization. Learn more.
09 Dec 2025	Feature	**StoreFront node relocation**	The **StoreFront** node has been removed from Web Studio. All settings and configuration options previously available in the **StoreFront** node are now available on the **Settings** tab of the **Delivery groups** node. This consolidation simplifies navigation and keeps related configuration options in one place. Learn more.
08 Dec 2025	Feature	**Machine hardware view in the Search node**	You can now access a dedicated hardware view in the Search node for machines provisioned using

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			Machine Creation Services (MCS). This view gives better visibility into machine hardware details and makes managing MCS-provisioned machines easier. Learn more.
08 Dec 2025	Feature	**Improved scope control for Default Policy Set**	Scope control has been available for policy sets. To maintain compatibility, **Default Policy Set** is now assigned to *any* scope, with **Bypass scope control** enabled by default. Review your **Default Policy Set** assignments and adjust them if you want to limit access based on scope. Learn more.
05 Dec 2025	Feature	**AWS EC2: Share prepared images across availability zones**	With this feature, you can share a single prepared image across different availability zones within the same AWS region for AWS EC2. This simplifies catalog creation and image updates, reducing management overhead

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			significantly. Currently, use PowerShell commands to manage image sharing. Learn more.
02 Dec 2025	Feature	**Create MCS provisioned VMs with vTPM enabled in XenServer 8**	With this feature in XenServer 8, you can create an MCS machine catalog with vTPM. If machine profile-based configuration is used and vTPM is enabled, then VMs in the catalog inherit the same vTPM content from the VM template. Learn more.
21 Nov 2025	Feature	**Amazon WorkSpaces Core Managed Instances: Share prepared images across availability zones using Studio UI**	With this feature, you can share a single prepared image across different availability zones within the same AWS region for Amazon WorkSpaces Core Managed Instances using Studio UI. Learn more.
20 Nov 2025	Feature	**One-time use pooled desktops in Local Host Cache**	You can now configure one-time use of pooled desktops during Local Host Cache (LHC) outage mode. It leverages a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			hygiene blob distributed only to VDAs version 2407 and later. Capable machines are automatically scheduled for reboot after a single outage session to guarantee a clean state. Learn more.
18 Nov 2025	Feature	**Managing prepared image versions in AWS EC2**	Image management functionality is now generally available for AWS EC2 virtualization environments. You can use **Images** node to create multiple image versions and apply or update multiple machine catalogs. Learn more.
17 Nov 2025	Feature	**Amazon WorkSpaces Core Managed Instances non-domain join support in Studio UI**	With this enhancement, you can provision Amazon WorkSpaces Core Managed Instances that are non-domain joined directly within the Studio UI using MCS. This functionality is supported during both the creation and editing phases of MCS machine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			catalogs in the Studio UI. Learn more.
07 Nov 2025	Feature	**Azure: Support cross-family backup VM sizes for Hibernated VMs**	MCS on Azure now supports using cross-family VM sizes for backup configurations in hibernation-enabled machine catalogs, improving resiliency. This feature removes the prior restriction that blocked cross-family fallback to prevent blue screen errors upon resume. Learn more.
30 Oct 2025	Feature	**Provision Persistent Workloads of Amazon WorkSpaces Core Managed Instances**	With this new capability, you can create a persistent catalog of Amazon WorkSpaces Core Managed Instances using MCS. User writes and changes to their desktops are persisted on the OS disk (root volume) between different boots of their persistent WorkSpaces Core Managed Instance provisioned by MCS. Learn more.
30 Oct 2025	Feature	**Amazon WorkSpaces Core**	With this feature, you can share a single

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		Managed Instances: Share prepared images across availability zones	prepared image across different availability zones within the same AWS region for Amazon WorkSpaces Core Managed Instances. This simplifies catalog creation and image updates, reducing management overhead significantly. Learn more.
30 Oct 2025	Feature	**Secure environment for AWS-managed traffic in Amazon WorkSpaces Core environment**	MCS enables network traffic (API calls from Citrix Cloud to AWS hypervisor) to be routed through Cloud Connectors in your Amazon WorkSpaces Core environment using Studio. Learn more.
30 Oct 2025	Feature	**Exclude maintenance mode VMs from the autoscale pool**	With the new desktop group property `PoolSizeExcludesMaintenanceMode`, you can now exclude VMs in maintenance mode from the autoscale pool irrespective of the delivery group. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
30 Oct 2025	Feature	**Share prepared image versions across clusters and vCenters**	You can now use the **Images** node to share image versions across hosting connections in VMware. This implementation ensures consistency and uniformity of images across different clusters or vCenters, enhancing deployment flexibility and operational efficiency. Learn more.
30 Oct 2025	Feature	**Citrix Advisor: New checks for reliability, performance, security, and cost efficiency**	Citrix Advisor now includes new environment checks that provide actionable recommendations to help improve reliability, performance, security, and cost efficiency. Learn more.
30 Oct 2025	Feature	**Enhanced user assignment default for improved security**	We've updated the default behavior when assigning users within a delivery group. Restricted control is now the default, ensuring better security and more granular access control. The

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			alternative option, **Allow any authenticated users to use resources**, is now clearly marked as **Not recommended**. Learn more.
30 Oct 2025	Feature	**Two new service health alerts**	Two new site-level alerts are available to help you monitor deployment health: **Resources are located in the initial zone** and **Advanced health check is not enabled on StoreFront.** To view these alerts, click the flag icon in the upper-right corner of the Home page. Learn more.
30 Oct 2025	Feature	**Improved application package management**	In Studio, you can now choose to automatically remove packages that no longer exist in the source (now called *Profile*) location when checking for updates. This new **Remove absent packages** option in the **Preferences** field helps you easily clean up the application packages UI by removing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			outdated entries from the **Packages** tab. Learn more.
24 Oct 2025	Feature	**Cross-account provisioning in AWS using Studio UI**	With this feature, Studio now supports cross-account provisioning in AWS. Learn more.
15 Oct 2025	Feature	**Enhanced proxy configuration for AWS host connections**	With this enhancement, AWS host connection can now read the WinHTTP system proxy value that is configured during Cloud Connector installation if you set the custom property `UseSystemProxyForHypervisorTrafficOnConnectors` to `true` when creating or updating a host connection using PowerShell. Learn more.
23 Sep 2025	Feature	**AWS Spot instance**	With this feature, you can create an MCS machine catalog of Spot instances (persistent request only) in AWS virtualization environment using machine profile workflow. Compared to On-demand instances, Spot

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			instances offer cost savings of up to 90%. Learn more.
23 Sep 2025	Feature	**Scoped Studio access for CSP tenant admins (Preview)**	As a Citrix Service Provider (CSP), you can now grant your tenant admins access to a lightweight version of the DaaS Studio console directly from their Citrix Cloud console. Learn more.
18 Sep 2025	Feature	**Citrix Troubleshoot Connection**	The Citrix Troubleshoot Connection feature is designed to empower end-users to effectively self-troubleshoot potential desktop or application launch failures. Learn more.
01 Sep 2025	Feature	**Image management in Red Hat OpenShift environments**	Image management functionality is now generally available for OpenShift virtualization environments. You can use **Images** node to create image definitions, versions, and MCS machine catalogs. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
13 Sep 2025	Feature	**Improved multi-selection in the Search node.**	We've updated the **Search** node with a more intuitive table layout. This change enables you to select multiple items using checkboxes in each row and select all items on the current page using the checkbox in the column header. Learn more.
01 Sep 2025	Feature	**Create Red Hat OpenShift catalogs using machine profile**	With this feature, using Studio, you can now create a Red Hat OpenShift catalog in MCS using a machine profile. The input of the machine profile is an existing VM. Learn more.
01 Sep 2025	Feature	**Managing prepared image versions in XenServer**	Image management functionality is now generally available for XenServer virtualization environments. You can use **Images** node to create multiple image versions, and apply or update to multiple machine catalogs. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
01 Sep 2025	Feature	**Improve upgrade reliability with a pre-upgrade VDA restart**	The VDA Upgrade Service now offers the ability to restart VDAs before the upgrade begins. This helps improve upgrade success rates by starting from a stable system state and avoiding issues caused by pending restarts. Learn more.
01 Sep 2025	Feature	**Secure Private Access integration in Web Studio**	The integration of Secure Private Access (SPA) with Web Studio is enhanced. Administrators in your organization can now open the SPA console directly from the left navigation in Web Studio. Learn more.
26 Aug 2025	Feature	**Multi-select support for delivery groups**	You can search for delivery group names using text input and multi-select up to 15 delivery groups for comprehensive analysis. Learn more.
21 Aug 2025	Feature	**Share prepared image versions across**	You can use the **Images** node to share image versions across hosting connections

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		subscriptions and tenants in Azure	in Azure. This implementation ensures consistency and uniformity of images across different subscriptions or tenants, enhancing deployment flexibility and operational efficiency. Learn more.
18 Aug 2025	Feature	**Connector Appliance health alerts**	This feature allows you to create and manage alerts for Connector Appliances. Learn more.
18 Aug 2025	Feature	**Improved handling of vertical and horizontal load balancing alerts**	This feature ensures that alerts only trigger for “Maximum capacity” in horizontal scaling scenarios. Learn more.
18 Aug 2025	Feature	**Enhanced network metrics collection for session troubleshooting**	This feature provides information on network metrics that are critical for Citrix session troubleshooting because session performance and stability depend heavily on underlying network conditions. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
11 Aug 2025	Feature	**Enhanced network metrics collection for session troubleshooting**	This feature provides information on network metrics that are critical for Citrix session troubleshooting because session performance and stability depend heavily on underlying network conditions. Learn more.
11 Aug 2025	Feature	**Observability for multi-session VDA**	The observability for multi-session VDA feature enhances the monitoring and troubleshooting capabilities for Secure Private Access sessions within a multi-user VDA environment. Learn more
08 Aug 2025	Feature	**Custom schedule for holidays**	Autoscale now allows you to create custom schedules to turn off unused VMs in a delivery group on specific days, like holidays, to reduce unnecessary resource consumption. Learn more
08 Aug 2025	Feature	**Image Management with Azure**	Use the **Images** node to prepare and manage images that are compatible with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		Confidential VMs using Studio UI	Azure Confidential VMs. Learn more
08 Aug 2025	Feature	**Enhanced mobile experience for critical on-the-go DaaS tasks**	You can now manage Citrix DaaS more easily from your mobile device. The updated experience is optimized for smaller screens, making it easier to access Studio from a mobile device when a desktop isn't available. Whether you're responding to an alert or quickly checking a misconfiguration, you can take action right away—no need to wait until you're back at your desk. Learn more
08 Aug 2025	Feature	**Customize your Studio view with My preferences settings.**	A new **My preferences** tab is now available under the **Settings** node. Settings on this tab let you tailor your Studio interface to suit your preferences. These settings apply only to your account and do not affect other administrators. Learn more

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
08 Aug 2025	Feature	**Improved restart UI for clearer control and customization**	We've enhanced the restart schedule UI to make restart modes clearer and more customizable. You can now easily distinguish between *graceful restart* and *forced restart*, and configure custom restart durations to suit your needs. Learn more
05 Aug 2025	Feature	**Citrix Advisor: Proactive insights and optimization for your DaaS deployment**	Citrix Advisor is a service that helps you optimize DaaS deployment and enhance its overall health and readiness. It automates environment checks and delivers actionable recommendations, empowering you to proactively identify configuration issues, inefficiencies, resource wastes, deviations from best practices, and more. Learn more
30 Jul 2025	Feature	**Cost summary**	This feature provides a comprehensive summary of the expenses associated with running the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			Citrix environments. Learn more
29 Jul 2025	Feature	**Cross-account provisioning in AWS**	This feature uses VPC peering and cross-account access using IAM roles to make provisioning across different AWS accounts possible for enterprises managing multiple AWS accounts. Learn more.
29 Jul 2025	Feature	**Backup SKU list for VMs in AWS**	With this feature, in the AWS virtualization environment, you can provide a list of backup EC2 instance types (Backup SKUs that can be On-demand instances) using PowerShell that MCS can fall back to in case of capacity-related issues. Learn more.
24 Jul 2025	Feature	**Enhanced session launch diagnostics with recommended actions**	The updated **Session Launch Failure Diagnostics** page offers a more thorough understanding of session launch issues. You can find the visualization of involved components

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			with error analysis and recommended actions. Learn more.
22 Jul 2025	Feature	**Integration with Nutanix Prism Central on AHV**	You can now connect Citrix DaaS to Nutanix AHV clusters through Nutanix Prism Central using a new host connection, Nutanix AHV Prism Central. Learn more.
21 Jul 2025	Feature	**MCS machine catalogs in Amazon Workspaces Core**	MCS has now integrated with Amazon Workspaces Core to provision non-persistent MCS machine catalogs in the customer's AWS account. Learn more.
21 Jul 2025	Feature	**Studio: Support for more granular control over access policies in delivery groups**	Previously, you could apply access policies to specific users only using PowerShell or REST APIs. Now, you can achieve this goal directly in Studio. This enhancement gives you more flexibility in defining different access conditions for various users or user groups, achieving more granular access control. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
21 Jul 2025	Feature	**Customize desktop icons across platforms using Studio**	Studio now allows you to customize desktop icons for any desktop of your choice. You can now upload icons and use them for desktops or apps, change the icon for individual desktops, or select from built-in icons for desktops of your choice. Learn more.
21 Jul 2025	Feature	**Option to use system proxy on Citrix Cloud Connectors for Redirected GCP API Traffic**	With this feature, you can redirect GCP API internet traffic on Citrix Cloud Connectors through the system proxy. This helps you to route all external traffic through a non-transparent proxy. Learn more.
21 Jul 2025	Feature	**Option to use system proxy on Citrix Cloud Connectors for Redirected Azure API Traffic**	With this feature, you can redirect Azure API internet traffic on Citrix Cloud Connectors through the system proxy. This helps you to route all external traffic through a non-transparent proxy. Learn more.
21 Jul 2025	Feature	**Share encrypted prepared image across**	With this feature, you can share an encrypted prepared

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		subscriptions and tenants for Azure	image across subscriptions and tenants. You can thereafter create a machine catalog in the resource where the encrypted prepared image is shared. Learn more.
21 Jul 2025	Feature	**Add notes while assigning prepared images**	With this feature, you can now add custom notes using Studio and PowerShell while creating or updating an MCS catalog with a prepared image. Learn more.
21 Jul 2025	Feature	**Azure Arc onboarding across all on-premises hypervisor**	With this feature, you can now enable Azure Arc Onboarding for an MCS machine catalog using PowerShell commands. Once onboarded, the VMs can be managed from the Azure portal to perform operations such as power management, add or remove extensions, assign policies, and enable Azure Monitor on the Arc-enabled VMs through built-in Azure policy. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
21 Jul 2025	Feature	**Migration from unmanaged to managed disks in Azure**	With this feature, you can migrate your MCS-provisioned Azure VMs from unmanaged to managed disks through Citrix. The migration applies to both persistent and non-persistent machine catalogs, supporting both on-demand and legacy VMs. Learn more.
21 Jul 2025	Feature	**Image Management with Azure Confidential VMs**	You can now prepare and manage images that are compatible with Azure Confidential VMs. Learn more.
18 Jul 2025	Feature	**Studio always-on mode**	Web Studio now introduces always-on mode to enhance resiliency and reduce downtime during infrastructure failures. In this read-only mode, you can securely view and monitor your Citrix DaaS environment even during service disruptions, helping maintain operational continuity. Always-on mode is available on all MANAGE nodes,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			except Quick Deploy. Learn more.
07 Jul 2025	Feature	**Studio: Support for managing Azure AD security groups using service accounts**	In Studio, you can now use Azure AD service accounts to configure and manage dynamic security groups for VMs. This update allows you to use a pre-configured service account to perform security group management without user interaction, simplifying the process and enhancing security. Learn more.
03 Jul 2025	Feature	**Display NVMe v6 SKUs for ephemeral OSDisk usage**	You now have the option to store an ephemeral OS disk on a NVMe Disk using Studio. Learn more.
03 Jul 2025	Feature	**Migrate existing MCS provisioned catalogs to prepared image machine catalog**	With this feature, you can convert an existing MCS catalog provisioned from master image to a catalog using a prepared image. Learn more.
03 Jul 2025	Feature	**Display NVMe v6 SKUs for**	You now have the option to store an ephemeral OS disk

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		ephemeral OSDisk usage	on a NVMe Disk using Studio. Learn more.
03 Jul 2025	Feature	**Option to use system proxy on Citrix Cloud Connectors for redirected Azure API Traffic**	With this feature, you can redirect Azure API internet traffic on Citrix Cloud Connectors through the system proxy. This helps you to route all external traffic through a non-transparent proxy. Learn more.
03 Jul 2025	Feature	**Option to use system proxy on Citrix Cloud Connectors for redirected GCP API Traffic**	With this feature, you can redirect GCP API internet traffic on Citrix Cloud Connectors through the system proxy. This helps you to route all external traffic through a non-transparent proxy. Learn more.
01 Jul 2025	Feature	**Monitor and troubleshoot Secure Private Access agentless apps in Monitor**	Administrators and help-desk personnel can now monitor and troubleshoot Secure Private Access agentless apps sessions and events in Monitor. Learn more.
01 Jul 2025	Feature	**Updated duration of Pending HA state**	The Pending HA state duration when Cloud Connectors

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			determine if there is a need to enter LHC mode has been extended from 60 to 90 seconds. Learn more.
26 Jun 2025	Feature	**Monitoring VDA logon duration details**	You can now view detailed information on VDA logon duration to provide visibility into the time taken to log on to the VDA. Learn more.
26 Jun 2025	Feature	**Endpoint metrics available on the Filters tab and Custom Reports**	You can now view additional endpoint metrics such as Public IP address, ISP, Location (Country or City), Workspace type - Citrix Workspace app (app or browser), and Access type (through Workspace or StoreFront) in the Monitor Connection or Session filters and Custom Reports. Learn more.
26 Jun 2025	Feature	**Bulk alert dismissal**	Allows administrators to bulk dismiss alerts by time, type or category, making it easier to manage alerts, especially during maintenance modes or when

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			dealing with alerts from hypervisors and other environments. Learn more.
26 Jun 2025	Feature	**Enhanced network metrics monitoring in Citrix Monitor**	Enhanced network metrics monitoring includes L7 latency monitoring, new network metrics, historical data, filtering options, and session connection path visualization for improved performance analysis and troubleshooting. Learn more.
26 Jun 2025	Feature	**Red Hat OpenShift virtualization environments**	With this feature, Citrix manages your Red Hat OpenShift workloads through a Citrix-managed OpenShift plug-in. Learn more
16 Jun 2025	Feature	**Improved UI performance for importing VMs from AWS**	Studio performance is now enhanced to optimize the process of importing VMs into Citrix DaaS from AWS. Learn more
11 Jun 2025	Feature	**Service account for routing Azure AD Identity traffic**	Using this feature, you can create and modify an Azure AD service account to route Azure AD identity traffic from

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			Delivery Controller to Azure AD through Citrix Cloud Connector to enhance security. Learn more
11 Jun 2025	Feature	**Assign security groups per network interface to VMs using the machine profile in AWS**	In the AWS virtualization environment, you can now create an MCS machine catalog where the provisioned VMs are assigned security groups per ENI (Network Interface). Learn more
06 Jun 2025	Update	**App packages**	Revamped App packages article. Learn more
06 Jun 2025	Feature	**Create host connections using Azure Managed Identity using Studio**	Using Studio, you can now create host connections to Microsoft Azure Resource Manager using Azure Managed Identity. This method offers a secure and scalable alternative to using a service principal, eliminating the need to manage credentials manually. Learn more
05 Jun 2025	Feature	**Cost modeling for Azure workloads**	The new cost modeling feature

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			supports Azure workloads and provides recommendations based on usage patterns. Learn more
05 Jun 2025	Feature	**Local application usage reporting**	With this feature, Citrix Monitor helps you to monitor the usage of applications launched within virtual desktop sessions (also known as local applications). Learn more
04 Jun 2025	Feature	**Support for assigning Citrix Group Policies to Microsoft Entra ID users**	You can now assign Citrix Group Policies to Microsoft Entra ID (Azure AD) users from multiple IDPs in Studio. Learn more.
04 Jun 2025	Feature	**View and filter machines by VDA upgrade state in Studio**	Studio now includes **VDA Upgrade State** as a column in the **Search** and **Machine Catalogs** nodes. This column shows the status of scheduled VDA upgrades—for example, whether an upgrade was successful. You can also filter machines based on their VDA upgrade state, making it easier to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			track and manage VDA upgrades across your deployment. Learn more
03 Jun 2025	Update	**Launch Hybrid Azure AD joined VDA sessions**	Removed the section as it is not supported. Learn more
02 Jun 2025	Feature	**Option to extend monitoring of HDX optimization beyond Microsoft Teams**	Adds an option to extend the monitoring of HDX optimization beyond Microsoft Teams. Learn more
02 Jun 2025	Feature	**New metrics in the Monitor dashboard**	Addition of new metrics—Total connected users and Citrix Workspace app versions—in the Citrix Monitor dashboard. Learn more
02 Jun 2025	Feature	**Enhancements to Cost savings page**	Addition of service provider filter, support for selecting multiple delivery groups, and enhanced visibility into failed machines. Learn more
28 May 2025	Feature	**Share encrypted prepared image across regions in Azure**	With this feature, you can share an encrypted prepared ACG image across multiple regions in the same

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			subscription and tenant using DES. You can thereafter create a machine catalog in the region where the encrypted prepared image is shared. Learn more
28 May 2025	Feature	**Update properties of individual VMs in VMware**	You can now update properties of individual VMs in a persistent MCS machine catalog using a PowerShell command. This implementation helps you to manage individual VMs efficiently without updating the entire machine catalog. Learn more
28 May 2025	Feature	**Support for updating MCS provisioned machines in VMware environments**	Using the PowerShell command `Set-ProvVMUpdateTimeWindow`, you can now apply the current provisioning scheme to an existing persistent or non-persistent machine or set of machines. This feature is applicable to machine profile and non-machine profile-based machine catalog. Learn more

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
27 May 2025	Feature	**Estimate Azure VM costs during catalog creation.**	When creating a machine catalog, you can now estimate the monthly cost of Azure virtual machines, including VM size and disk costs. You can also refine the estimate by adjusting settings such as daily power-on hours, workdays, savings plans, reserved instances, and shutdown storage. Learn more
27 May 2025	Feature	**Visualization of provisioning cost insights.**	You can now view detailed cost information for machine catalogs. The visualization provides an overview of provisioning costs and trends for the last 30 days. Learn more
27 May 2025	Feature	**Support for converting catalogs from using master images to using prepared images.**	With a new action, **Convert to Prepared Image**, in Studio, you can now convert MCS-provisioned machine catalogs using master images to catalogs using prepared images. This feature is available for Azure and VMware

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			virtualization environments. Learn more
26 May 2025	Feature	**Proxy configuration for service accounts**	Service accounts creation now supports proxy configuration through NGS Proxy for Azure AD Identity management. Learn more
15 May 2025	Feature	**Connector Appliance health metrics**	Enables customers to monitor Connector Appliance's health under the Infrastructure monitoring dashboard. Learn more
06 May 2025	Feature	**Use Autoscale to hibernate VMs**	The power management is now enhanced to support hibernation of VMs through Autoscale configurable settings using PowerShell. Learn more
29 Apr 2025	Feature	**Intelligent Autoscale schedules plugin**	Intelligent Autoscale is a data driven Autoscale feature with minimum administrative settings that allows you to configure the performance target of a delivery group. The performance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			target value ranges from 1 to 99 and the value specifies a target balance between user experience and cost. Learn more
29 Apr 2025	Update	**Use persistent desktops with a non-persistent user profile in Citrix for Amazon WorkSpaces Core**	Added the setting to use persistent desktops with a non-persistent user profile in Citrix for Amazon WorkSpaces Core. Learn more
29 Apr 2025	Update	**Additional Cloud Connector configuration when using Rendezvous V1**	Added the setting to have additional Cloud Connector configuration when using Rendezvous V1. Learn more
28 Apr 2025	Feature	**Studio: Studio: Support for exercising access control over apps at the delivery group level.**	You can now perform access control over apps at the delivery group level. Currently, this ability is limited to controlling access to all apps within a delivery group. Learn more.
28 Apr 2025	Feature	**Client Platform filter for policy assignments.**	You can now control policy assignments more precisely with a new filter, Client Platform. This filter lets you assign

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			(Allow) or exclude (Deny) policies based on the operating system of users' devices, including Windows, macOS, Linux, iOS, Android, or HTML5. This enhancement offers greater flexibility and precision in policy assignment, ensuring a customized and uniform experience across managed and unmanaged devices. Learn more.
28 Apr 2025	Feature	**Option to reset In-Use Active Directory (AD) accounts.**	With Studio you can now reset machine Active Directory (AD) accounts even when the status of the machine is In Use. Learn more.
28 Apr 2025	Feature	**Support for provisioning Data disk in VMware**	With this feature, you can now create and assign a persistent and non-persistent Data disk to an MCS created persistent or non-persistent VM of an MCS machine catalog in VMware. Learn more
28 Apr 2025	Feature	**Enable trusted launch of existing**	With this feature, you can update an

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		persistent and non-persistent catalogs	existing non-Trusted Launch persistent and non-persistent machine catalog to a catalog enabled with Trusted Launch. Learn more
28 Apr 2025	Feature	**Simplified Azure AD security group management using service accounts**	With this enhancement, MCS now supports using a pre-created service account to manage Azure AD security groups for Azure AD joined machines. Learn more
28 Apr 2025	Feature	**Support for SCVMM 2025**	Citrix DaaS now supports Microsoft's System Center Virtual Machine Manager (SCVMM) 2025. Learn more
28 Apr 2025	Feature	**Create Hybrid Azure AD joined catalogs and Hybrid Azure AD joined catalogs enrolled in Microsoft Intune with prepared images**	With this feature, you can now use prepared images to create Hybrid Azure AD joined catalogs and Hybrid Azure AD joined catalogs enrolled in Microsoft Intune using Studio and PowerShell commands. Learn more
23 Apr 2025	Feature	**Support for automatically using Azure Temporary**	When you edit an MCS-provisioned catalog in Studio, the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
		Disk for write-back cache disk.	catalog now automatically uses Azure Temporary Disk for the write-back cache (WBC) disk if the required criteria are met. As a result, new VMs added to the catalog uses Azure Temporary Disk for the WBC disk. Learn more
22 Apr 2025	Feature	**App visibility control support for Azure AD users.**	With Studio, you can now control which Azure AD users and groups can see a specific app in the Workspace app. Learn more.
28 Mar 2025	Update	**Remove broker user from the cache**	Added article on removing broker user from the cache. Learn more.
27 Mar 2025	Feature	**Re-trust option for untrusted host connection certificates.**	If a host connection outage occurs due to an untrusted certificate, you can re-trust the certificate for that host connection in Studio. Learn more
27 Mar 2025	Feature	**Re-sync deployments in AWS UI.**	A new option to re-sync deployments in AWS is added. Re-sync a deployment that is in Pending

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			state or if the number of machines listed in a deployment does not match with the number of machines listed in AWS. Learn more
27 Mar 2025	Feature	**Centralized site management is generally available.**	As a Cloud Administrator of multiple sites, you can now designate one site as the primary and link other sites to it for streamlined, centralized management. This feature helps improve operational efficiency by reducing the need to switch between sites for daily tasks. Learn more
27 Mar 2025	Feature	**UI Enhancements in Studio.**	You can now copy data directly from tables and use table pagination for improved performance and usability. Learn more
27 Mar 2025	Feature	**What's new widget enhancement.**	You can now switch between **Featured** for curated feature insights and **General** for comprehensive DaaS feature updates. Learn more

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
27 Mar 2025	Feature	**Token usage limit in token-based enrollment increased to 5000.**	We've increased the token usage limit in token-based enrollment from 100 to 5000, allowing for greater flexibility when enrolling machines in large-capacity machine catalogs. Learn more
26 Mar 2025	Feature	**Migration of non-persistent VMs in VMware**	With this feature, you can migrate non-persistent VM disks from one storage to another storage using the `Move-ProvVMDisk` PowerShell command. Learn more.
26 Mar 2025	Feature	**Migration of VMs in XenServer**	With this feature, you can migrate persistent and non-persistent VM disks from one storage to another storage using the `Move-ProvVMDisk` PowerShell command. Learn more.
20 Mar 2025	Update	**Added Applications article**	Added Applications article in Citrix DaaS document. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
17 Mar 2025	Feature	**Enhanced Autoscale features for improved power management**	We've enhanced Autoscale to improve your experiences. Learn more.
12 Mar 2025	Feature	**Improvement to Workload rightsizing**	You can now use the **Workload rightsizing** (formerly Infrastructure Rightsizing) tab to identify power users. Learn more.
12 Mar 2025	Feature	**Enhancement to Session Performance tab**	You can now use the **Session Performance** tab to view details on protocol, MS teams, HDX connection type, input frames per second, and output frames per second. Learn more.
07 Mar 2025	Update	**Load balance machines**	Revamped load balancing article. Learn more
07 Mar 2025	Feature	**Security groups configurations are inherited from machine profiles**	You can now create an MCS machine catalog and select a machine profile that has security groups assigned. This avoids the security group configuration as it is inherited from the machine profile. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
06 Mar 2025	Feature	**Autoscale holiday plug-in**	With this feature, you can deviate from the standard Autoscale settings related to the power management of VMs and allow VMs to be powered off on specified holiday dates. Learn more.
06 Mar 2025	Feature	**Match UEFI boot program to Citrix Provisioning version**	This feature ensures that for Citrix Provisioning catalogs created using MCS, the target devices boot from the latest boot settings file, ensuring that target devices align with the Citrix Provisioning version. Learn more
05 Mar 2025	Feature	**Create Azure AD joined and Microsoft Intune enrolled catalogs with prepared images**	With this feature, you can now use prepared images to create Azure Active Directory joined and Microsoft Intune enrolled catalogs using Studio and PowerShell commands. Learn more
05 Mar 2025	Feature	**Flexible storage location option for VMs**	This feature gives you the ability to balance VM allocation across different storage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			service using the Enhanced current round robin allocation method and Least load-based allocation method. Learn more
05 Mar 2025	Feature	**Enhanced resource monitoring for multi-session VDAs in Studio**	Studio now provides detailed resource utilization and capability insights for multi-session VDAs. Hover over the **Load Evaluator Index** column of a multi-session VDA in the **Search** node to view detailed metrics. Learn more
05 Mar 2025	Feature	**Improved session visibility in tag-based searches**	When you search for *machines* by tag in **Studio > Search**, active user *sessions* on the matching machines now appear on the **Sessions** tab. This enhancement helps prevent accidental shutdowns of machines with active sessions by providing clear visibility of those sessions. Learn more

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
28 Feb 2025	Feature	**Support for provisioning data disk on Azure**	You can now create and assign a persistent data disk to an MCS created persistent or non-persistent VM of an MCS machine catalog in Azure. The data disk is used for storage of persistent data like event logs, security traces, and application data. Learn more
27 Feb 2025	Feature	**Navigate seamlessly from Studio to Monitor for machines and sessions**	A new option, **View in Monitor**, is now available in **Studio > Search**, providing quicker access to detailed session and machine information in **Monitor**. Learn more
26 Feb 2025	Feature	**Cost Savings by optimizing storage usage**	The **Cost Savings** page is enhanced with visibility into the amount of savings achieved through storage optimization when machines are powered Off. Learn more
25 Feb 2025	Feature	**NitroTPM and UEFI secure boot for MCS created AWS VM instances**	In AWS environments, you can now select a master image (AMI) enabled with NitroTPM and/or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			UEFI secure boot. This implementation ensures that the VMs are secured and trusted. Learn more
25 Feb 2025	Update	**Monitor action enhancements**	You can now use a progress bar for actions and support to limit action scope based on user roles. Learn more
24 Feb 2025	Update	**Limits**	Updated the limits of the number of VDAs and application groups. Learn more
20 Feb 2025	Update	**Whitelisted urls**	Updated Remote PowerShell SDK whitelisted urls. Learn more
18 Feb 2025	Update	**Option to view and troubleshoot Secure Private Access Sessions for hybrid deployments.**	This enhancement allows DaaS customers using Gateway, StoreFront, and Secure Private Access on-premises to monitor and troubleshoot their session data directly in the DaaS Monitor. Learn more.
11 Feb 2025	Feature	**Share prepared image versions across hosting units in VMware**	You can now use the **Images node** to share image versions across hosting units within the same hosting connection in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			VMware. You can also use PowerShell commands to achieve this goal. Learn more
05 Feb 2025	Feature	**Support for creating MCSIO-enabled MCS machine catalogs in AWS**	. You can now create MCSIO-enabled MCS catalogs to create MCSIO-enabled MCS machine catalogs in AWS to improve write IOPS by directing write operations to the write-back cache and to reduce the startup time when the persisting OS disk is enabled. Learn more
30 Jan 2025	Feature	**Integration with Webhook**	Citrix Monitor now integrates with Webhook, allowing you to create webhook profiles for tools like Slack, Microsoft Teams, and ServiceNow from the **Alerting and ITSM** section on the **Integrations and data exports** page. Learn more.
24 Jan 2025	Update	**Secure Boot and vTPM**	Updated the article to emphasize that vTPM is not a requirement for Secure Boot and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			added content for XenServer. Learn more
22 Jan 2025	Feature	**Filter master images based on hosting unit regions**	During machine catalog creation for the Azure platform, Studio can now filter out and exclude master images that belong to different regions other than the hosting unit region. This ensures that only images from the same region as the hosting unit are available for selection. Learn more.
21 Jan 2025	Feature	**Add applications to existing AWS deployments in Quick deploy node**	You can now add applications to existing AWS deployments thus simplifying the overall deployment process. Learn more.
21 Jan 2025	Feature	**Option to reset In-Use Active Directory (AD) accounts**	With Studio you can now reset machine Active Directory (AD) accounts even when the status of the machine is In -Use.
21 Jan 2025	Feature	**Alerting admins that power policies remain effective when disabling Autoscale™**	The enhancement is to remind the admins that disabling Autoscale does not affect the power

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			policy settings for a delivery group. This ensures that admins are aware of the scope of Autoscale disabling and clarifies that power policies remain effective when Autoscale is turned off.
20 Jan 2025	Feature	**MCSIO with only disk cache no longer supported**	The option to configure MCSIO with only disk cache (without memory cache) has been removed across all hypervisor and cloud service environments. Learn more
20 Jan 2025	Feature	**Creating AWS VMs using machine template properties no longer supported**	The **Apply machine template properties to virtual machines** option has been removed from the **Machine Template** page. Instead, create AWS VMs using machine profiles for a similar and more streamlined experience. Learn more
20 Jan 2025	Feature	**Create MCSIO enabled catalog in AWS**	With this feature, you can create an MCSIO enabled non-persistent catalog in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			AWS using PowerShell commands. MCSIO improves the performance of the VM by caching disk operations in either memory or on a small, high-speed disk. The option to configure MCSIO with only disk cache (without memory cache) using Studio has been removed across all hypervisors and cloud service environments. Learn more
17 Jan 2025	Feature	**Least used and unused published apps report**	With this feature, you can view detailed usage information for published apps accessed through Citrix Workspace app, which helps you to optimize app management and resource allocation. Learn more
16 Jan 2025	Feature	**Secure Private Access integration with Monitor (Preview)**	With this feature, you can monitor and troubleshoot all Secure Private Access sessions in Monitor. Learn more

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
15 Jan 2025	Update	Local Host Cache	Updated the entire article to improve accuracy. Learn more
26 Dec 2024	Update	Removal of Preview tag from Cost summary page	Removed the Preview tag from the **Cost savings** feature as the feature has been released for general availability. Learn more
24 Dec 2024	Feature	**Automated configuration tool cmdlets for backup and restore**	With this feature, you can use PowerShell commands supported by the automated configuration tool to trigger the backup and restore APIs that Studio uses. Learn more
20 Dec 2024	Update	Installation considerations	Removed the reference to CTX139030 and redirected to System requirements
16 Dec 2024	Feature	**Optimize storage load balancing with the least load method**	With this enhancement, Studio has introduced the **Optimize storage load balancing with least load method** option. If you select two or more OS data storage locations during catalog

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			creation, this option becomes available, enabling disks to be allocated to the least loaded storage repository. Learn more
13 Dec 2024	Feature	**Secure Private Access tab on Monitor**	With this feature, Citrix Monitor provides a dedicated place for all new features related to Secure Private Access. Learn more
13 Dec 2024	Feature	**Visibility for Secure Private Access Service**	With this feature, Citrix Monitor provides detailed monitoring and visibility for Secure Private Access applications and users. Learn more#visibility-for-secure-private-access-service
13 Dec 2024	Feature	**Unified platform experience for Citrix Monitor**	With this feature, Citrix Monitor now aligns with all other components within Citrix Cloud, providing a unified platform experience. Learn more
13 Dec 2024	Feature	**Enhancement to Connections tab**	With this enhancement, the **Connections** tab in Citrix Monitor now

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			offers streamlined navigation for quicker troubleshooting. Learn more
13 Dec 2024	Feature	**Filter resource location details**	With this feature, Citrix Monitor allows you to view the resource location for single-session or multi-session OS machines in the **Filters** > **Machines** tab. Learn more
13 Dec 2024	Feature	**Enhancement to Session Performance tab**	With this feature, you can use the **Session Performance** tab in Citrix Monitor to monitor additional endpoint metrics which exist in the Citrix Workspace app for Windows, Mac, Linux, HTML5, or Chrome. Learn more
13 Dec 2024	Feature	**Machine net active usage**	With this feature, you can use the **Workload rightsizing** page in Citrix Monitor to get detailed insights into machine net active usage. Learn more
13 Dec 2024	Feature	**Cloud Connector health monitoring**	With this feature, you can monitor the health of Cloud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			Connectors using a single dashboard view and proactively configure alerts. Learn more
10 Dec 2024	Feature	**NVMe-only SKUs**	With this feature, MCS supports the NVMe storage controller type for the new VM SKUs on Azure. You can create an MCS machine catalog using a service offering that supports only NVMe or both SCSI and NVMe. Learn more
10 Dec 2024	Feature	**Set a default time zone for your site**	With Studio, you can now set a default time zone for your Citrix DaaS site. Studio uses this time zone for all time displays and scheduling such as scheduled restart and autoscaling. Learn more
10 Dec 2024	Feature	**Studio adopts Citrix Cloud unified navigation**	As part of the shift towards a unified navigation experience across the Citrix Cloud platform, we've updated Studio to align with this

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TITLE	DESCRIPTION
			platform-wide initiative. Learn more
06 Dec 2024	Feature	**AWS on-demand provisioning**	With AWS on-demand provisioning, the OS disk gets deleted when you shut down a non-persistent VM. This implementation saves cost when the VM is not in use. Learn more
03 Dec 2024	Feature	**Show Secure Default Settings**	This feature shows the secure default setting along with the default setting for a policy. The default setting might be overwritten by the secure default setting. Learn more

© 1997–2026 Citrix Systems, Inc. All rights reserved.